#ibminterconnect

SHARE
Educate · Network · Influence

There's a new Sheriff in Town
CICS Policy Based Management

Steve Zemblowski
zem@us.ibm.com

CELEBRATING 60 ★YEARS★ OF SHARE
Influencing IT Since 1955

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence.**

SHARE in Seattle 2015

Session Abstract

My systems work perfectly—it's the applications that are the problem!" If you have ever said (or thought) that, then this session is for you.

Outages do not have to be "an application issue" anymore. In CICS TS 5, new policy-based capabilities allow you to set thresholds on the resources that your applications are allowed to consume. Rogue applications can be detected through various task threshold policies, such as excessive file or database access, repetitive program links, or abnormal storage requests. Once detected, you have the ability to notify, to react, or to ABEND.

There's a new sheriff in town, and it's you. Come to this session to learn how to exercise your new power wisely.

Session Agenda

- CICS Policy Based Management
- Resources
- Actions
- Policy Scope
- Summary

Notes

This session will cover CICS Policy Based Management. We will discuss the resources one can put a threshold on and the actions one can take when a threshold is exceeded. The session will also cover how to scope the policy. In other words how to have the policy apply to a CICS regions, a Platform, a specific Application or an operation within an Application.

CICS Policies

- Can control the behavior of Applications and Platforms
- Define threshold conditions to manage user tasks
  - Monitor the resource usage of a task
  - Automatically take action when threshold is exceeded
- Detection of looping or runaway tasks
- A condition and action pair make up a policy rule
  - Multiple rules can be defined in a policy
- Policies are defined in a CICS bundle
  - Multiple policies can be in a single bundle

Notes

- The behavior of applications and platforms can be controlled during run time, based on predefined policies. CICS® performs the action that is specified in the policy when tasks that are running exceed defined thresholds for resource usage.
- Policies define threshold conditions that manage the behavior of user tasks within CICS regions. Policies contain one or more rule types with associated thresholds and actions. You can deploy policies to monitor the resource utilization of a user task, and to automatically respond when resource usage exceeds the thresholds you define. In this way, excessive resource usage and looping and runaway transactions can be detected and dealt with appropriately.

CICS Policies…

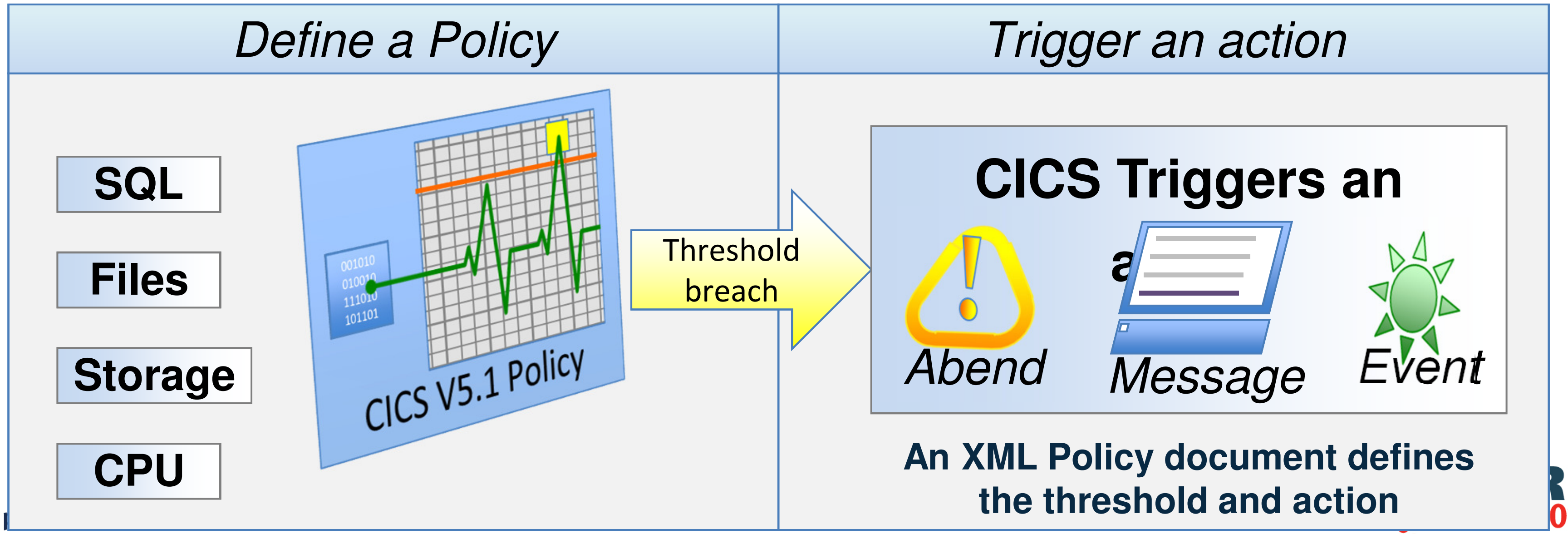
- Available Actions
  - Issue a message
    - DFHMP3001
  - Emit an Event
  - Abort the task
    - Abend code AMPB or user specified

Notes

- CICS® monitors task resource utilization and if any thresholds, as defined by any deployed policies, are exceeded, CICS performs the specified action. The actions that can be performed when a threshold is exceeded are: Issue the message DFHMP3001, which is the default policy action. This message is issued so that the system programmer can take the appropriate action.
- Abend the task. The task is ended by CICS, message DFHMP3002 is issued, and either the default abend code AMPB or a user-specified abend code is issued. By default a transaction dump is taken for the abend. You can suppress the transaction dump or request a system dump by using the CEMT SET TRDUMPCODE|SYDUMPCODE and EXEC CICS SET TRANDUMPCODE|SYDUMPCODE commands. You can handle the abend by using the EXEC CICS HANDLE ABEND command.
- Emit an event. The user can specify the name of either an EP adapter or EP adapter set. The event has the same behavior as CICS system events, and as with system events, a policy event can be emitted to only an asynchronous and non-transactional EP adapter. The information that is captured in the event is pre-determined and non-customizable.

CICS Policies…

- Policy Based Management
  - Condition and action
  - Action can be:
    - Emit a message
    - Emit a system event
    - Abend the task



An XML Policy document defines the threshold and action

Notes

- Managed operations are provided through the introduction of policies, which deliver automated control over critical system resources
- A new, dynamic policy-based management capability is introduced in support of both applications and platforms. Policies enable the behavior of applications and platforms to be managed by determining whether tasks running as part of a platform, as an application, or as types of operation within an application, exceed certain predefined thresholds.
- Task thresholds can be set based on data access requests, storage usage, program loops and processor time used. For example, a threshold could be defined based on the amount of above-the-line storage used by a task, the number of times a task accesses IBM DB2 or a file, or the number of EXEC LINK requests issued by a user task.
- After a threshold is exceeded, CICS can issue a message, or abend the task with a specific abend. Additionally, policies can be defined to trigger one or more CICS events, which can in turn initiate other actions.
- CICS policies are a declarative way of ensuring that applications and platforms continue to run effectively. A policy can be applied to any combination of applications and platforms. Additionally, policies can also be deployed into a single region, independently of defining a platform. Policies are applied dynamically during production operations.

Policy Rule Types

- Database request
- File request
- Program request
- Start request
- Storage request
- Syncpoint request
- Transient Data request
- Temporary Storage request

Notes

You can define threshold conditions to limit the following requests made by CICS user tasks:

CICS TS 51 introduced these thresholds:

The amount of task or shared storage below the line (24-bit), above the line (31-bit), or above the bar (64-bit).

The number of requests for task or shared storage below the line (24-bit), above the line (31-bit), or above the bar (64-bit).

The number of EXEC CICS LINK or EXEC CICS INVOKE APPLICATION requests.

The number of EXEC SQL requests.

The number of EXEC CICS file access requests, that is: READ, READ UPDATE, WRITE, REWRITE, DELETE, STARTBR, READNEXT, or READPREV requests.

The amount of CPU time that is consumed by a task.

CICS TS 52 added these thresholds:

The elapsed time that is taken by a task.

The number of EXEC CICS READQ or WRITEQ TS requests for main or auxiliary temporary storage queues.

The amount of data that is written to main or auxiliary temporary storage queues by EXEC CICS WRITEQ TS requests.

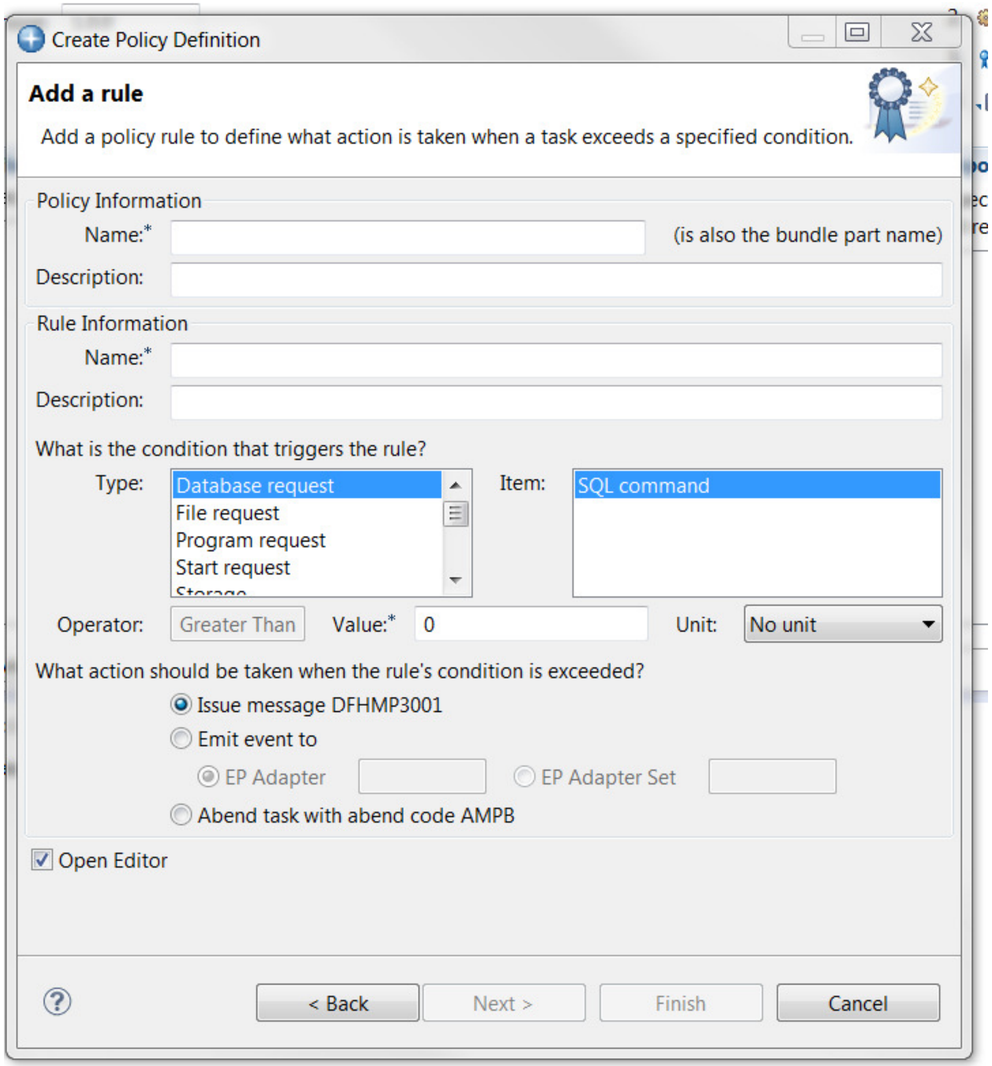
The number of EXEC CICS SYNCPOINT requests.

The number of EXEC CICS START requests.

The number of EXEC CICS READQ or WRITEQ TD requests.

Database

- Define a threshold for the number of SQL requests
  - Includes requests issued in exits
    - e.g. CICS VSAM Transparency



Create Policy Definition

Add a rule

Add a policy rule to define what action is taken when a task exceeds a specified condition.

Policy Information

Name:* (is also the bundle part name)

Description:

Rule Information

Name:*

Description:

What is the condition that triggers the rule?

Type: Database request / File request / Program request / Start request / Storage

Item: SQL command

Operator: Greater Than Value:* 0 Unit: No unit

What action should be taken when the rule's condition is exceeded?

● Issue message DFHMP3001

○ Emit event to

○ EP Adapter ○ EP Adapter Set

○ Abend task with abend code AMPB

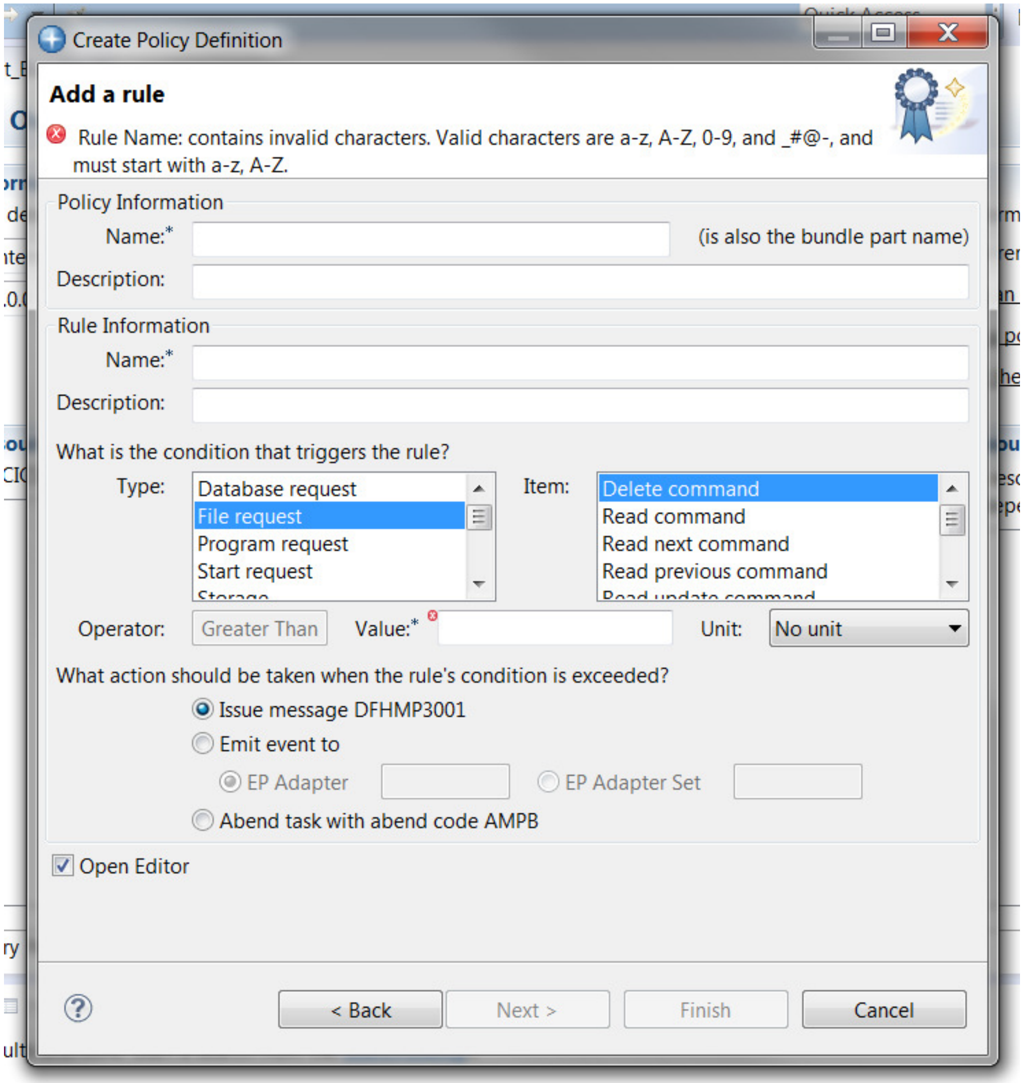
☑ Open Editor

Notes

- **Database request**
- Use the database request policy rule type to define a threshold for the number of DB2® SQL requests performed by a user task, and take automatic action if the threshold is exceeded. The count includes SQL requests issued by exits. For example, a program that issues EXEC CICS FILE requests that are converted into SQL requests by CICS® VT counts both towards any file request threshold and any SQL count threshold.

File

- Define a threshold for the number of FILE requests
  - Applies to a specific file command
  - Not a cumulative count
  - Counted whether the command is successful of not
  - Counted for the user task in the AOR whether the file is local or remote



Add a rule

Rule Name: contains invalid characters. Valid characters are a-z, A-Z, 0-9, and _#@-, and must start with a-z, A-Z.

Policy Information

Name:* (is also the bundle part name)

Description:

Rule Information

Name:*

Description:

What is the condition that triggers the rule?

Type: Database request / **File request** / Program request / Start request / Storage

Item: **Delete command** / Read command / Read next command / Read previous command / Read update command

Operator: Greater Than Value:* Unit: No unit

What action should be taken when the rule's condition is exceeded?

● Issue message DFHMP3001

○ Emit event to

● EP Adapter ○ EP Adapter Set

○ Abend task with abend code AMPB

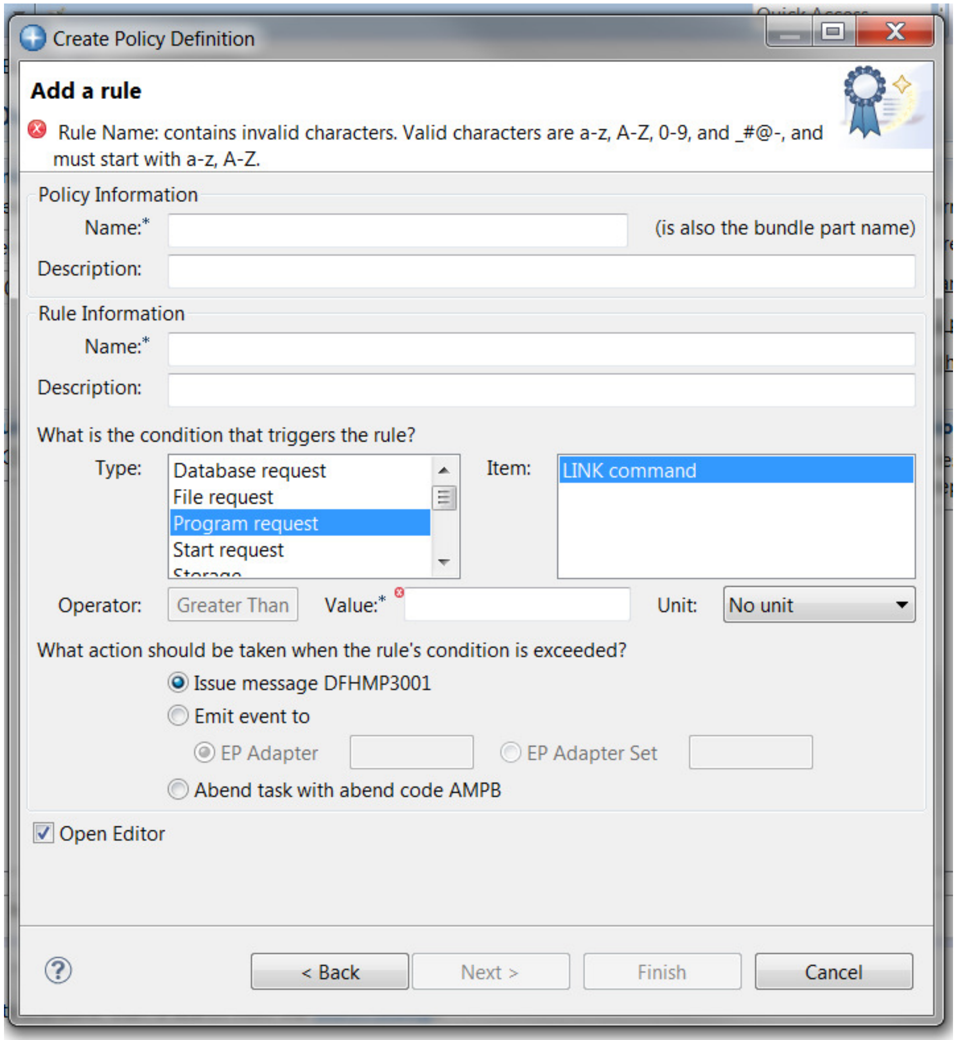
☑ Open Editor

Notes

- **File request**
- Use the file request policy rule type to define a threshold for the number of EXEC CICS file access requests performed by a user task, and take automatic action if the threshold is exceeded. The threshold applies to a specific file command, for example READ. It is not a cumulative count of all file access requests. File requests are counted when an application makes a file control request, whether the request is successful or not, including when an XFCREQ global user exit returns a response code of UERCBYP (ignore request). Requests are counted under the task for the application-owning region (AOR), whether the file is local or remote. Requests are not counted in the file-owning region (FOR).

Program

- Define a threshold for the number of LINK requests
  - Includes a count of the INVOKE APPLICATION requests



Create Policy Definition

Add a rule

Rule Name: contains invalid characters. Valid characters are a-z, A-Z, 0-9, and _#@-, and must start with a-z, A-Z.

Type: Program request

Item: LINK command

Operator: Greater Than

Unit: No unit

● Issue message DFHMP3001

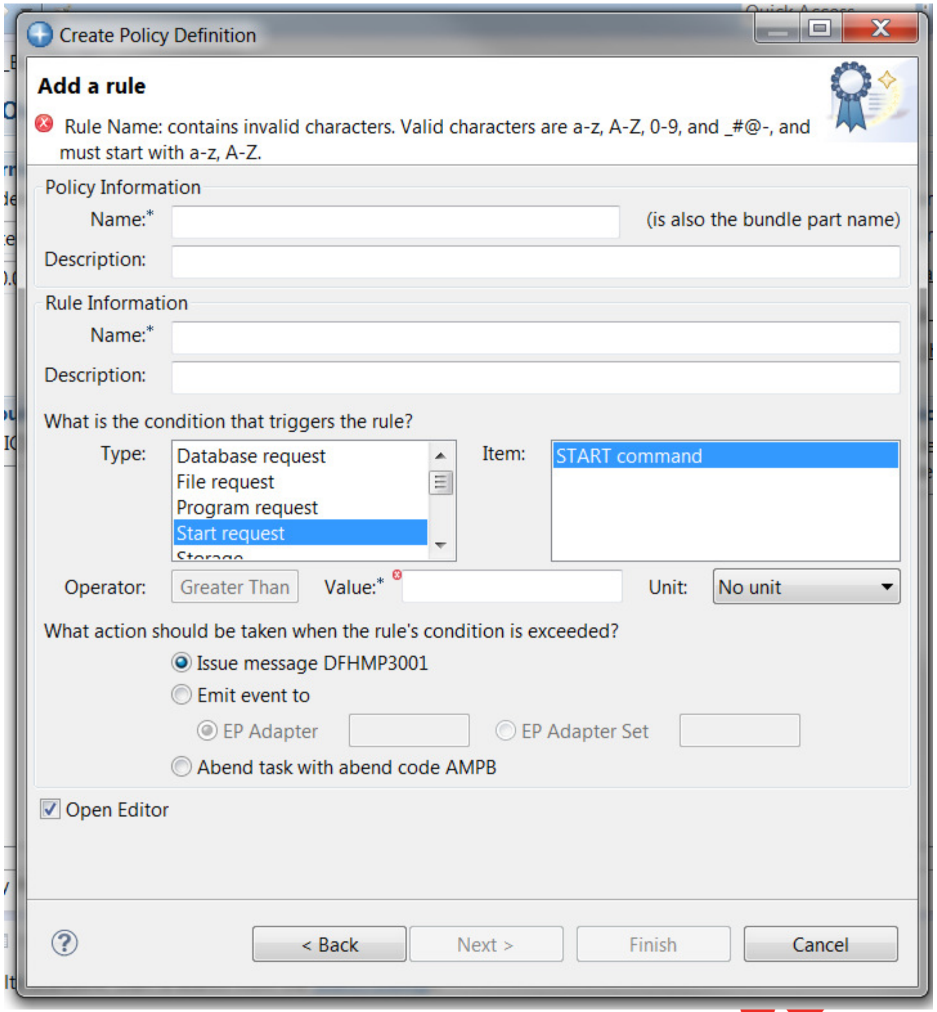
☑ Open Editor

Notes

- **Program request**
- Use the program request policy rule type to define a threshold for the number of EXEC CICS LINK or EXEC CICS INVOKE APPLICATION requests that are performed by a user task, and take automatic action if the threshold is exceeded. This rule type applies to requests that are serviced locally or remotely, whether successful or not, including when an XPCREQ global user exit returns a response code of UERCBYP (ignore request). Any task that is started in a remote region that services a DPL request is then outside of the scope of the rules that are applied to the task that issued the DPL, so any further requests that the remote task might perform are not counted by the local task.
- Note: EXEC CICS INVOKE APPLICATION requests are included in the count for EXEC CICS LINK requests; they cannot be counted separately.

Start

- Define a threshold for the number of START requests
  - Request counted whether successful or not
    - e.g. XICREQ returns an IGNORE response
    - e.g. XICERES returns a resource not available response



Create Policy Definition

Add a rule

Rule Name: contains invalid characters. Valid characters are a-z, A-Z, 0-9, and _#@-, and must start with a-z, A-Z.

Policy Information

Name:* (is also the bundle part name)

Description:

Rule Information

Name:*

Description:

What is the condition that triggers the rule?

Type: Database request, File request, Program request, **Start request**, Storage

Item: **START command**

Operator: Greater Than Value:* Unit: No unit

What action should be taken when the rule's condition is exceeded?

● Issue message DFHMP3001

○ Emit event to

○ EP Adapter ○ EP Adapter Set

○ Abend task with abend code AMPB

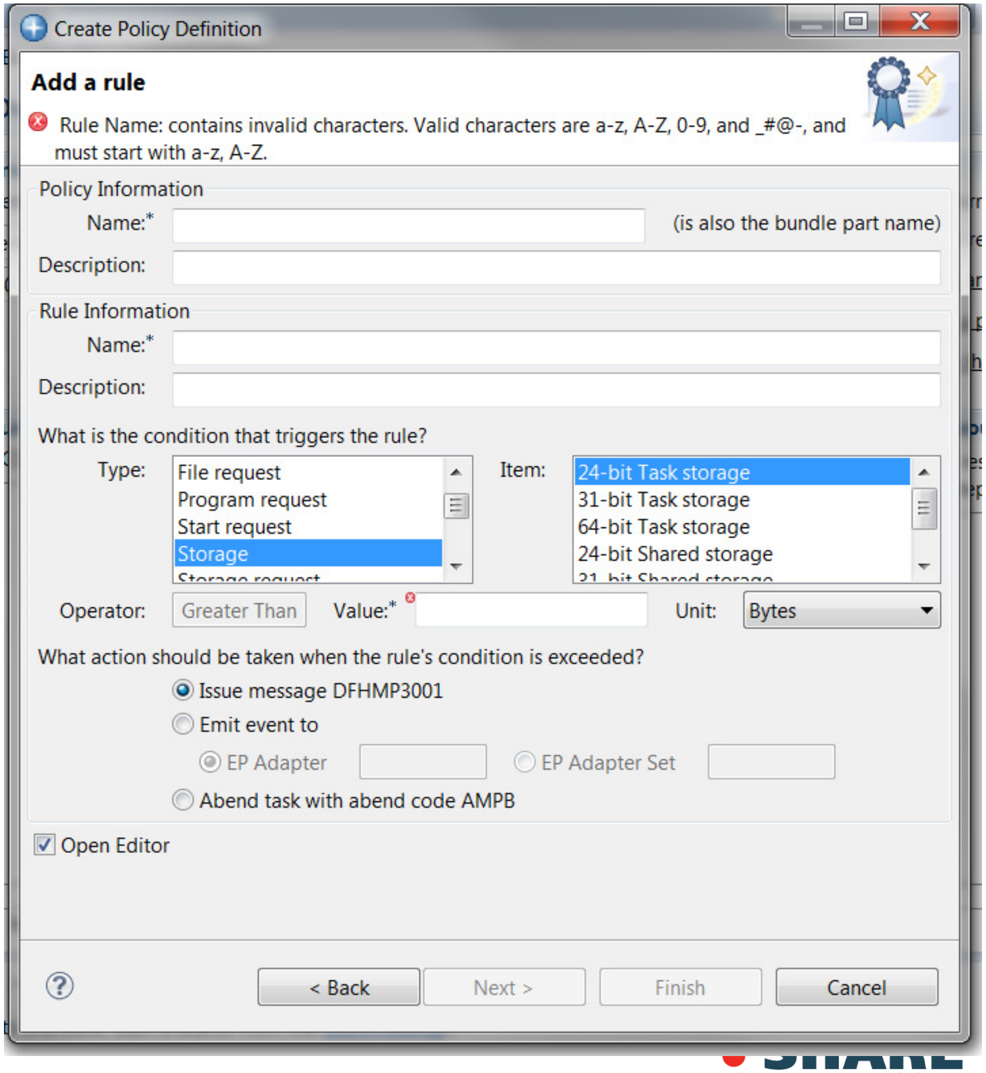
☑ Open Editor

Notes

- **Start request**
- Use the start request policy rule type to define a threshold for the number of EXEC CICS START requests that are performed by a user task, and take automatic action if the threshold is exceeded. All EXEC CICS START requests are counted whether the request is successful or not, including when an XICREQ global user exit returns a response code of UERCBYP (ignore request), or when an XICERES exit returns a response code of UERCPURG (a required resource is unavailable). Note: When you are using a policy on function-shipped EXEC CICS START requests in a remote region, the trigger mechanism depends on the interregion communication protocol and settings.

Storage

- Define a threshold for the amount of STORAGE allocated to the user task
  - Count includes all GETMAIN requests for a task
    - Explicit and Implicit
  - Count is decremented when an explicit or implicit FREEMAIN is issued
    - Not for SHARED storage



Create Policy Definition

Add a rule

Rule Name: contains invalid characters. Valid characters are a-z, A-Z, 0-9, and _#@-, and must start with a-z, A-Z.

Policy Information

Name:* (is also the bundle part name)

Description:

Rule Information

Name:*

Description:

What is the condition that triggers the rule?

Type: File request, Program request, Start request, **Storage** (selected), Storage request

Item: **24-bit Task storage** (selected), 31-bit Task storage, 64-bit Task storage, 24-bit Shared storage, 31-bit Shared storage

Operator: Greater Than Value:* Unit: Bytes

What action should be taken when the rule's condition is exceeded?

● Issue message DFHMP3001

○ Emit event to

● EP Adapter ○ EP Adapter Set

○ Abend task with abend code AMPB

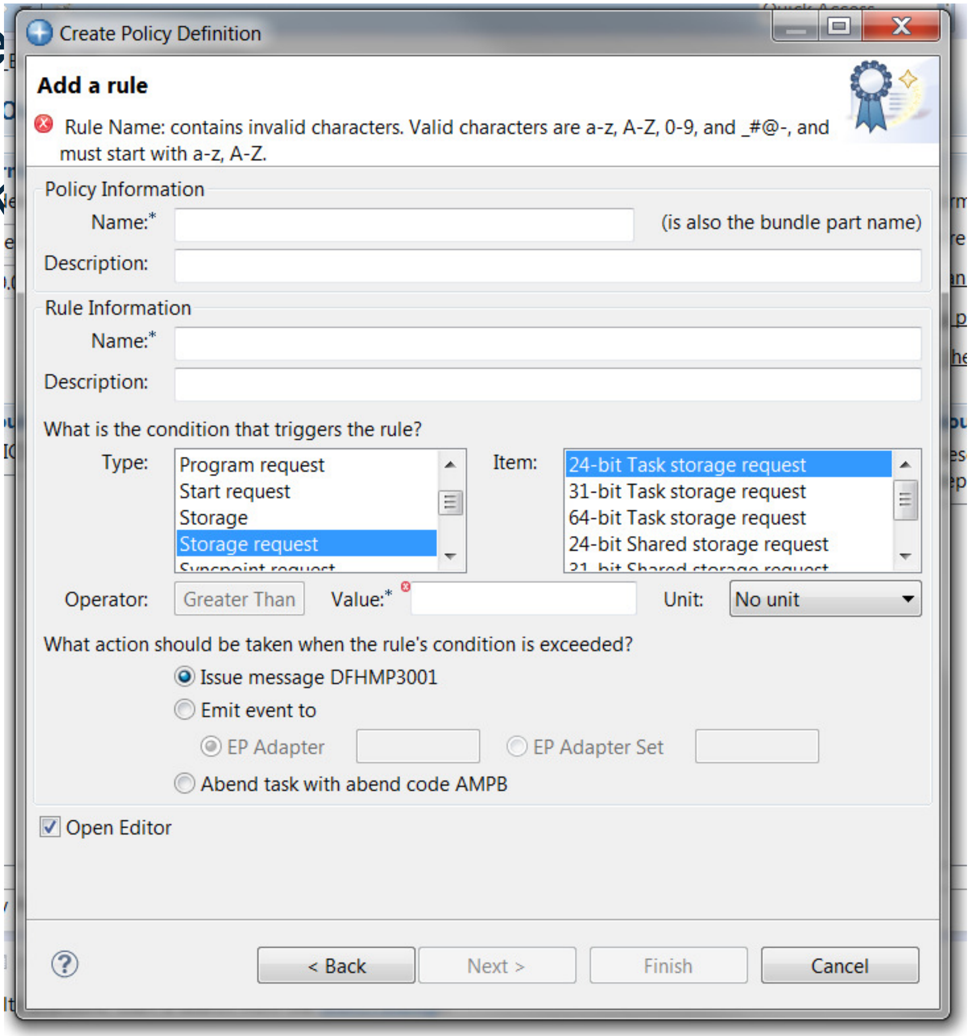
☑ Open Editor

Notes

- **Storage**
- Use the storage policy rule type to define a threshold for the amount of storage that is allocated by a user task, and take automatic action if the threshold is exceeded. The threshold applies to a specific storage class, for example 31-bit task storage. It is not a cumulative count of all storage requests.
- The threshold count includes all GETMAIN requests performed by a user task: both explicit EXEC CICS GETMAIN requests and implicit GETMAIN requests that occur in response to other EXEC CICS commands, for example EXEC CICS READ FILE SET. For task-related storage requests (task24, task31, and task64) the count is decremented when the task issues an explicit or implicit FREEMAIN. However, the counts for shared storage (shared24, shared31, and shared64) are NOT decremented when a task releases shared storage.
- Important: If an EXEC CICS GETMAIN with the NOSUSPEND option satisfies a rule that specifies an action of event, the task might be suspended during capture of the event data.

Storage Requests

- Define a threshold for the number of STORAGE requests for the user task
  - Count includes all requests for a task
    - Explicit and Implicit
      - e.g. EXEC CICS READ FILE SET



Create Policy Definition

Add a rule

Rule Name: contains invalid characters. Valid characters are a-z, A-Z, 0-9, and _#@-, and must start with a-z, A-Z.

Policy Information

Name:* (is also the bundle part name)

Description:

Rule Information

Name:*

Description:

What is the condition that triggers the rule?

Type: Program request / Start request / Storage / **Storage request** / Syncpoint request

Item: **24-bit Task storage request** / 31-bit Task storage request / 64-bit Task storage request / 24-bit Shared storage request / 31-bit Shared storage request

Operator: Greater Than Value:* Unit: No unit

What action should be taken when the rule's condition is exceeded?

● Issue message DFHMP3001

○ Emit event to

● EP Adapter ○ EP Adapter Set

○ Abend task with abend code AMPB

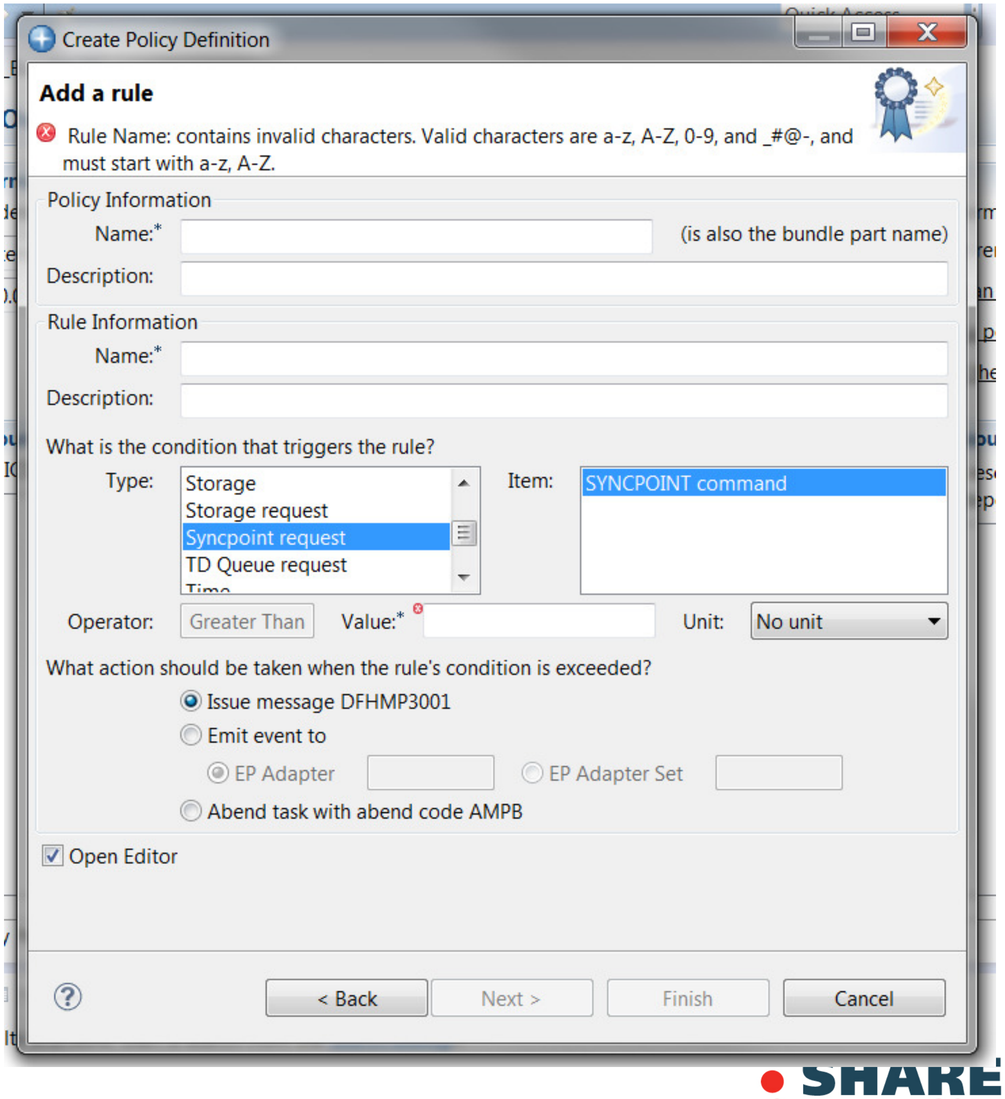
☑ Open Editor

Notes

- **Storage request**
- Use the storage request policy rule type to define a threshold for the number of GETMAIN requests performed by a user task, and take automatic action if the threshold is exceeded. This differs from the storage policy rule type, which is used to define thresholds that are based on the amount of storage allocated. The storage request threshold count contains the number of all GETMAIN requests performed by a user task: both explicit EXEC CICS GETMAIN requests and implicit GETMAIN requests that occur in response to other EXEC CICS commands, for example EXEC CICS READ FILE SET.
- Important: If an EXEC CICS GETMAIN with the NOSUSPEND option satisfies a rule that specifies an action of event, the task might be suspended during capture of the event data.

Syncpoint

- Define a threshold for the number of SYNCPOINT requests for the user task
  - ROLLBACK is included in the count



Rule Name: contains invalid characters. Valid characters are a-z, A-Z, 0-9, and _#@-, and must start with a-z, A-Z.

Policy Information

Name:* (is also the bundle part name)

Description:

Rule Information

Name:*

Description:

What is the condition that triggers the rule?

Type: Storage / Storage request / Syncpoint request / TD Queue request / Time

Item: SYNCPOINT command

Operator: Greater Than Value:* Unit: No unit

What action should be taken when the rule's condition is exceeded?

● Issue message DFHMP3001

○ Emit event to

● EP Adapter ○ EP Adapter Set

○ Abend task with abend code AMPB

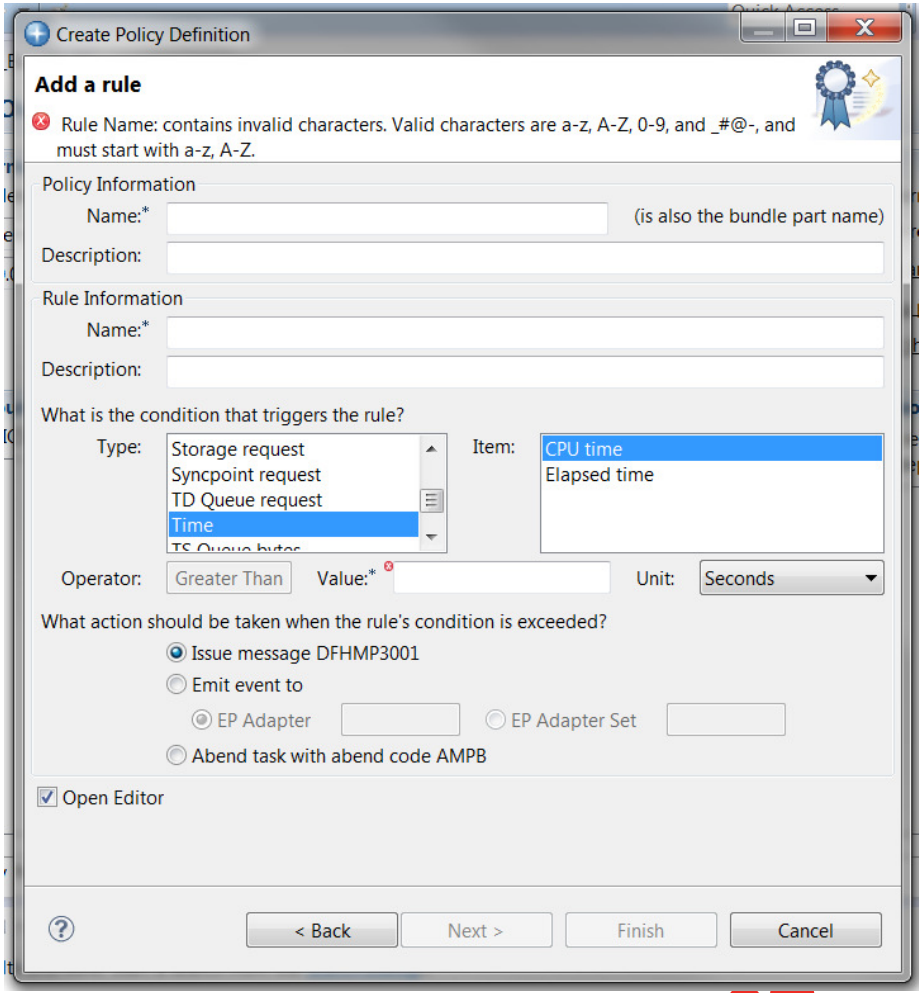
☑ Open Editor

Notes

- **Syncpoint request**
- Use the syncpoint request policy rule type to define a threshold for the number of EXEC CICS SYNCPOINT requests that are performed by a user task, and take automatic action if the threshold is exceeded. EXEC CICS SYNCPOINT and SYNCPOINT ROLLBACK requests are both counted, and unsuccessful requests are included in addition to successful requests.

Time

- Define a threshold for the amount of TIME consumed by a user task
  - CPU Time
    - Check is made when a task gives up control
    - Use RUNAWAY controls to detect a tight loop
  - ELAPSED Time
    - Check is made when a task issues an EXEC CICS command or invokes a TRUE
      - ABEND action will be taken after the command completes



Add a rule

Rule Name: contains invalid characters. Valid characters are a-z, A-Z, 0-9, and _#@-, and must start with a-z, A-Z.

Policy Information

Name:* (is also the bundle part name)

Description:

Rule Information

Name:*

Description:

What is the condition that triggers the rule?

Type: Storage request, Syncpoint request, TD Queue request, **Time** (selected), TS Queue bytes

Item: **CPU time** (selected), Elapsed time

Operator: Greater Than Value:* Unit: Seconds

What action should be taken when the rule's condition is exceeded?

● Issue message DFHMP3001

○ Emit event to

○ EP Adapter ○ EP Adapter Set

○ Abend task with abend code AMPB

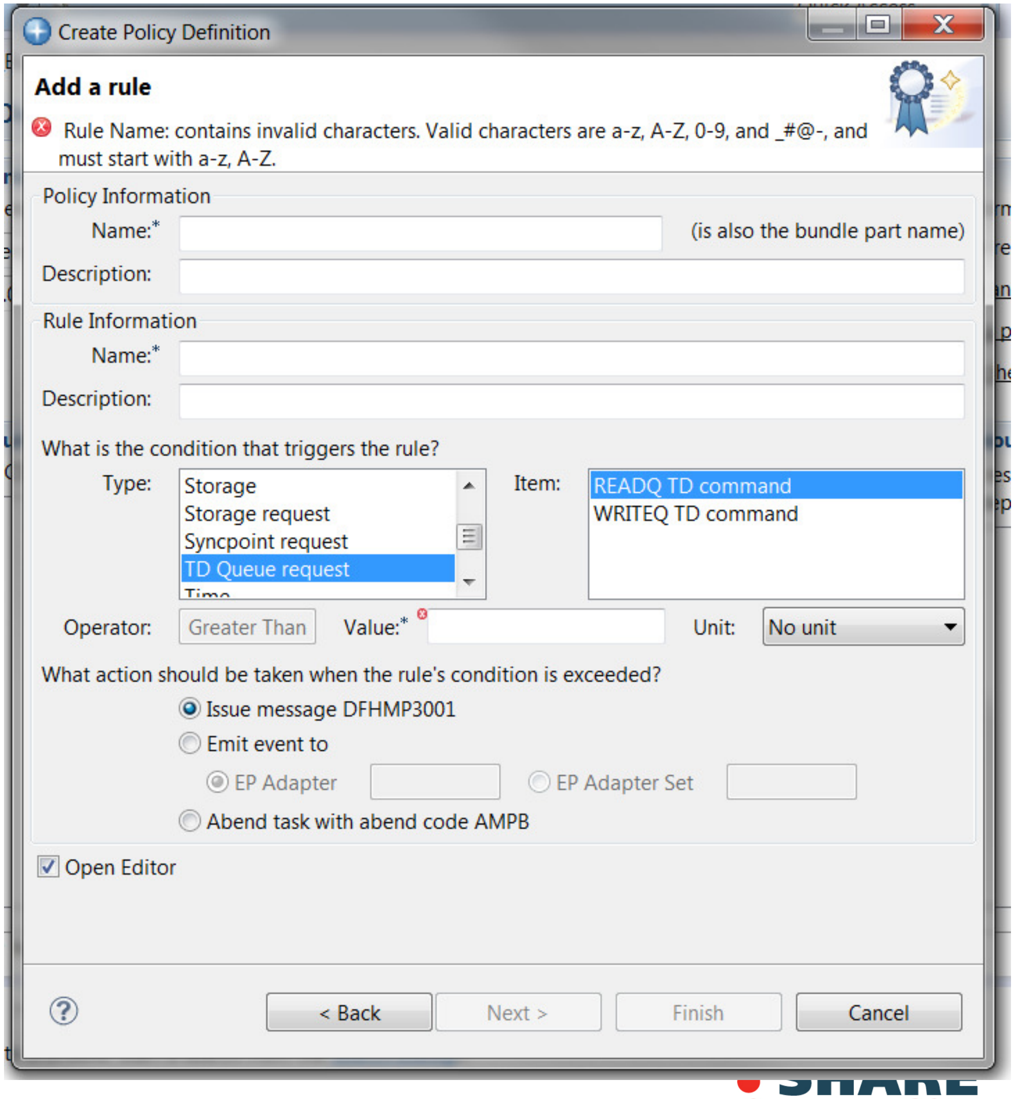
☑ Open Editor

Notes

- **Time**
- Use the time policy rule type to define a threshold for the amount of processor time that is used by a user task (CPU time policy item), or the amount of elapsed time that is taken by a task (Elapsed time policy item), and take automatic action if the threshold is exceeded. The time policy rule type differs from the other policy rule types in that the threshold is based on time, rather than a count of API requests, or the amount of storage allocated.
- Note: For the CPU time policy item: Due to the way processor changes are recorded, it is not possible to count the processor time continually, so on occasions the threshold might be exceeded sometime before it is detected by this function, and if you were to compare monitoring data with policy threshold actions taken, you might see some discrepancy. The CPU time policy item compares the total processor time with the policy threshold value. However, the processor time value is not incremented until a task gives up control of a processor, so a task might greatly exceed a threshold before it gives up control of the processor and allows the check to occur.
- For CPU time policy items, it is not until the task is redispatched and next issues an EXEC CICS call or calls a TRUE (for example an EXEC SQL call) that it checks whether the CPU time threshold is exceeded. If, for some reason, the task never gives up control, normal RUNAWAY processing abends the task when the RUNAWAY time interval is exceeded, before any time policy processing occurs. For Elapsed time policy items, a check whether the elapsed time threshold is exceeded is made every time a task issues an EXEC CICS call or calls a TRUE. In either case if the threshold is exceeded and the rule action is abend, the abend happens after the command completes.

Transient Data

- Define a threshold for the number of TRANSIENT DATA requests for the user task
  - Be aware other products write to Transient Data
    - Language Environment for diagnostic information
    - TCP/IP Socket Interface for CICS



Create Policy Definition

Add a rule

☒ Rule Name: contains invalid characters. Valid characters are a-z, A-Z, 0-9, and _#@-, and must start with a-z, A-Z.

Policy Information

Name:* (is also the bundle part name)

Description:

Rule Information

Name:*

Description:

What is the condition that triggers the rule?

Type: Storage / Storage request / Syncpoint request / **TD Queue request** / Time

Item: **READQ TD command** / WRITEQ TD command

Operator: Greater Than Value:* Unit: No unit

What action should be taken when the rule's condition is exceeded?

● Issue message DFHMP3001

○ Emit event to

○ EP Adapter ○ EP Adapter Set

○ Abend task with abend code AMPB

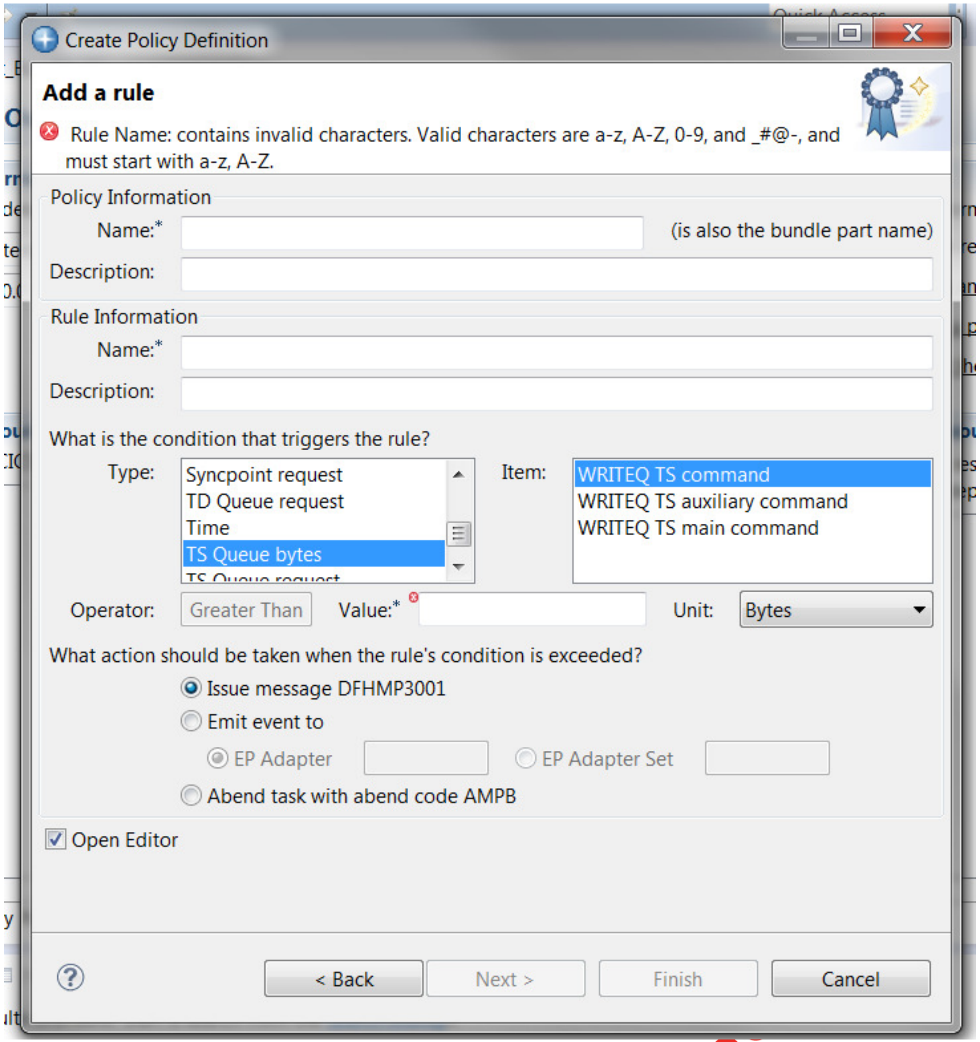
☑ Open Editor

Notes

- TD Queue request
- Use the TD Queue request policy rule type to define a threshold for the number of transient data queue (TDQ) access requests that are performed by a user task, and take automatic action if the threshold is exceeded. Both EXEC CICS READQ TD and EXEC CICS WRITEQ TD requests are counted, and every request is counted whether successful or not, including when an XTDREQ global user exit returns a response code of UERCBYP (ignore request).
- Note: A number of products write to the CICS TDQ, which might lead to a higher number of requests than you expect. For example, Language Environment uses EXEC CICS WRITEQ TD extensively for writing diagnostic information, as well as capturing output from cobol display and C printf() statements. IP CICS Sockets is another product that uses EXEC CICS WRITEQ requests.

Temporary Storage Bytes

- Define a threshold for the amount of data written to TEMPORARY STORAGE by a user task
  - Both WRITEQ TS and REWRITE TS are counted
  - REWRITE TS count is the total size of the rewrite, not the delta



Create Policy Definition

Add a rule

Rule Name: contains invalid characters. Valid characters are a-z, A-Z, 0-9, and _#@-, and must start with a-z, A-Z.

Policy Information

Name:* (is also the bundle part name)

Description:

Rule Information

Name:*

Description:

What is the condition that triggers the rule?

Type: Syncpoint request / TD Queue request / Time / **TS Queue bytes** (selected) / TS Queue request

Item: **WRITEQ TS command** (selected) / WRITEQ TS auxiliary command / WRITEQ TS main command

Operator: Greater Than Value:* Unit: Bytes

What action should be taken when the rule's condition is exceeded?

● Issue message DFHMP3001

○ Emit event to

○ EP Adapter ○ EP Adapter Set

○ Abend task with abend code AMPB

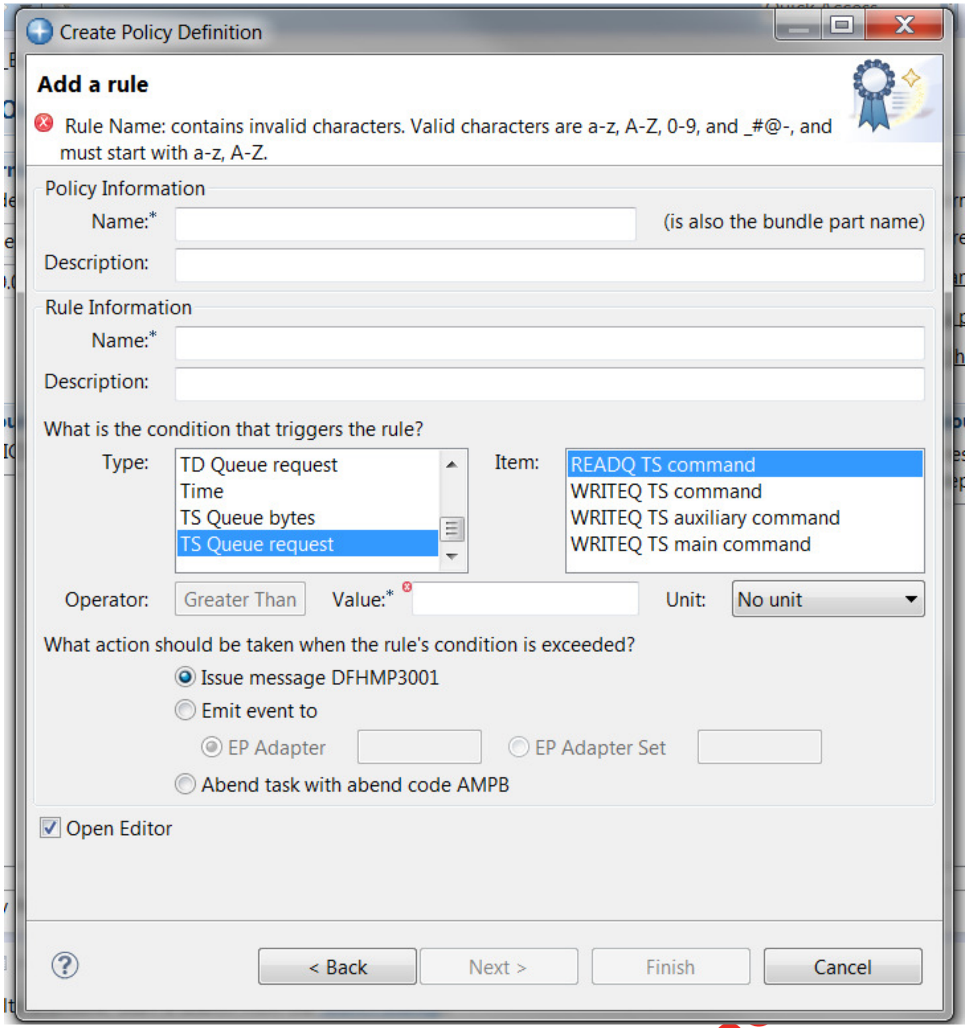
☑ Open Editor

Notes

- **TS Queue bytes**
- Use the TS Queue bytes policy rule type to define a threshold for the total amount of data that is written by a user task to either an individual temporary storage queue (TSQ) type (either auxiliary or main), or to the total amount of data that is written to the auxiliary and main TSQs combined, and take automatic action if the threshold is exceeded. Data from only successful requests is counted. Data that is written by both EXEC CICS WRITEQ TS and EXEC CICS WRITEQ TS REWRITE requests count towards the total. For EXEC CICS WRITEQ TS REWRITE requests the count is incremented by the total size of the REWRITE, and not the delta between the original WRITE and REWRITE. This behavior is consistent with the way the MN Domain treats TSQ WRITE and REWRITE requests.

Temporary Storage

- Define a threshold for the number of TEMPORARY STORAGE requests by a user task
  - REWRITE TS is counted as a WRITEQ
  - Request are counted whether successful or not
  - Synchronous events to temporary storage are counted



Create Policy Definition

Add a rule

Rule Name: contains invalid characters. Valid characters are a-z, A-Z, 0-9, and _#@-, and must start with a-z, A-Z.

Policy Information

Name:* (is also the bundle part name)

Description:

Rule Information

Name:*

Description:

What is the condition that triggers the rule?

Type: TD Queue request / Time / TS Queue bytes / TS Queue request (selected)

Item: READQ TS command (selected) / WRITEQ TS command / WRITEQ TS auxiliary command / WRITEQ TS main command

Operator: Greater Than Value:* Unit: No unit

What action should be taken when the rule's condition is exceeded?

● Issue message DFHMP3001

○ Emit event to

○ EP Adapter ○ EP Adapter Set

○ Abend task with abend code AMPB

☑ Open Editor

Notes

- **TS Queue request**
- Use the TS Queue request policy rule type to define a threshold for the number of EXEC CICS READQ TS and EXEC CICS WRITEQ TS requests that are issued by a user task to auxiliary or main temporary storage queues (TSQ), or to all auxiliary and main TSQs combined, and take automatic action if the threshold is exceeded. Requests to read or write local shared temporary storage queues are NOT counted. All TSQ access requests to auxiliary and main TSQs are counted whether successful or not, including when an XTSEREQ global user exit returns a response code of UERCBYP (ignore request). EXEC CICS WRITEQ TS REWRITE requests are counted as WRITEQ.
- Note: The following points apply to both the TS Queue bytes and the TS Queue request policy rule types: For remote TSQ requests, only the aggregate READQ TS and WRITEQ TS counts are updated, but this will include shared TSQ requests. As the TSQ type for a remote request is not known in the AOR, the counts for specific queue types are not updated. TSQ requests issued by programs that are invoked by distributed program link (DPL) or tasks started by transaction routing are counted in the remote system (AOR) only.
- TSQ requests issued by CICS system code as an indirect result of something that is triggered by a CICS user task might be counted. For example, the Temporary Storage Event adapter DFHECEAT issues TSQ requests if a user task triggers a CICS event. If the event is defined as SYNChronous, then these requests are issued under the capturing (user) task and get counted by policy code. If the event is asynchronous, the TSQ requests are issued under a CICS system task (and one whose initial program starts DFH) so a policy does not apply to that task and they are not counted.
- TSQ requests issued by CICS that do not go through the CICS EXEC interface program (DFHEIP) are counted by monitoring but not by policy code.

Policy Exceptions

- Policies do not apply to:
  - CICS system tasks
    - Includes CPLT at systems initialization
  - All terminal initiated CICS supplied transactions
    - Except CECI
  - All user tasks started by event processing
  - All non-terminal CICS supplied transactions
    - Except:
      - All web interface tasks
      - All CICS MQ bridge tasks
      - All CICS mirror transactions
      - All Liberty initiated transactions
      - All CICS pipeline tasks

Notes

- Policies are used to manage the behavior of user tasks. They do not apply to the following tasks: All CICS system tasks. This includes the CPLT system task under which CICS initialization PLT programs run.
- All terminal initiated CICS supplied transactions, except CECI.
- All user tasks started by event processing, for example, tasks started by Start Transaction adapters.
- All non-terminal initiated CICS supplied transactions, except for those in the following list.
- Policies do apply to the following non-terminal initiated CICS supplied transactions: All Web interface tasks, that is, transactions whose initial program is DFHWBA, except for the CMCI transaction CWWU.
- All CICS WebSphere® MQ bridge tasks, that is, transactions whose initial program is either DFHMQBP0 or DFHMQBP3, for example the CKBP and CKBC transactions.
- All CICS mirror transactions, that is, transactions whose initial program is DFHMIRS.
- All Liberty initiated transactions, that is, transactions whose initial program is DFHSJTHP.
- All CICS Pipeline tasks, that is, transactions whose initial program is DFHPIDSH (the SOAP HTTP Inbound Router program), DFHPIDSQ (the SOAP MQ Inbound Router program), or DFHPILSQ (the SOAP MQ Inbound Listener program).

Policy Scope

- Policies are deployed to a specific scope
  - Application scope
  - Operation within an application scope
  - Platform scope
  - No scope (e.g. Region scope)

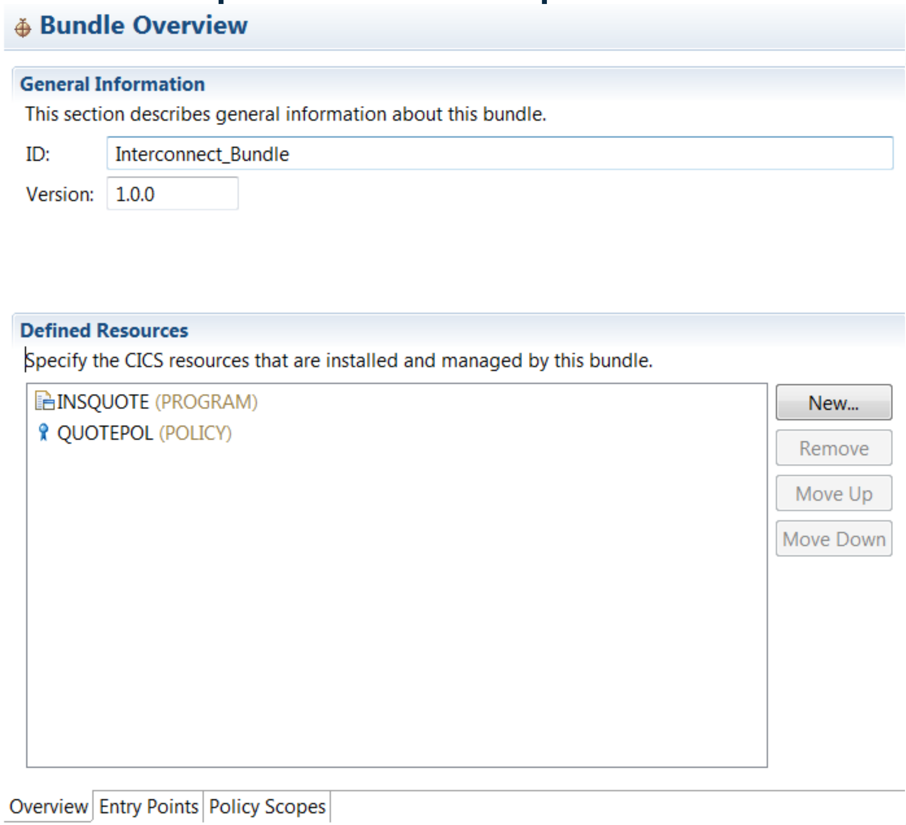
- Policies are defined in CICS bundles
  - Scope is determined by where the bundle is deployed
    - Platform: packaged as part of the platform and deployed during platform installation
    - Application: packaged as part of the application and deployed when the application is installed
    - Operation: policy associated with the entry point (operation)
    - Region: defined in the CSD and installed in any CICS region

Notes

- Policies are defined in CICS® bundles. The scope of a policy describes how it is applied to CICS user tasks.
- Policies are deployed to a specific scope. The scope can be either a region scope, a platform scope, an application scope, or an operation (within an application) scope.
- When a policy is deployed with a platform scope, it applies to all user tasks within the platform that have the matching platform in their application context. When a policy is deployed with an application scope, it applies to all user tasks within the platform that have the matching platform, application, and application version information in their application context. When a policy is deployed with an operation scope, it applies only to user tasks that also match the operation.
- A policy can also be deployed with region scope, in which case it applies to all user tasks that are running in that CICS region. This method is useful in a stand-alone CICS region (SMSS) where you are not able to define a platform and applications.

Policy Scope…

- Associating a policy with an operation
  - A PROGRAM or URIMAP can be an entry point and thus provide an operation to which policy can be applied



Bundle Overview

General Information

This section describes general information about this bundle.

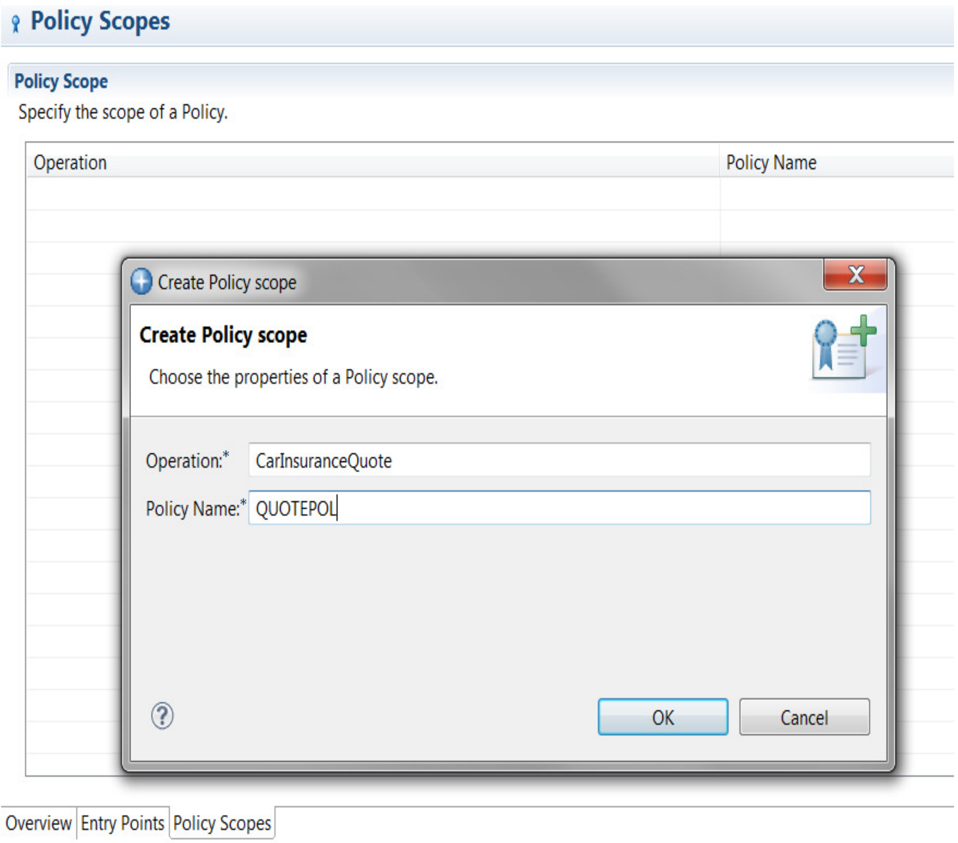
ID: Interconnect_Bundle

Version: 1.0.0

Defined Resources

Specify the CICS resources that are installed and managed by this bundle.

- INSQUOTE (PROGRAM)
- QUOTEPOL (POLICY)



Policy Scopes

Policy Scope

Specify the scope of a Policy.

Operation	Policy Name

Create Policy scope

Choose the properties of a Policy scope.

Operation:* CarInsuranceQuote

Policy Name:* QUOTEPOL

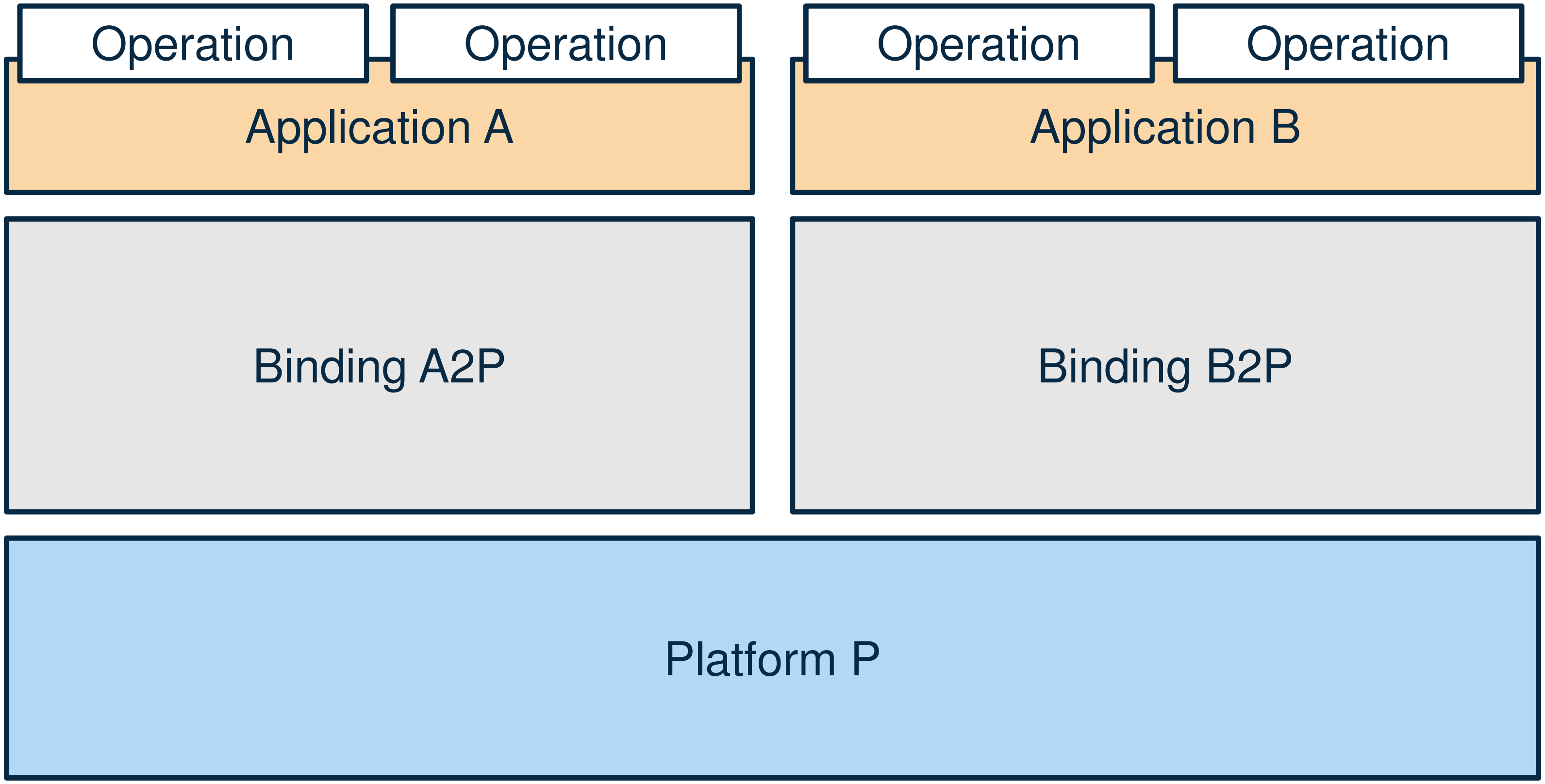
Notes

- PROGRAM and URIMAP resources can be identified as application entry points.
- For applications that are deployed on a platform, application entry points control users' access to the different versions of the application. Application entry points can be set as available or unavailable to users. You can install the application and its resources in the CICS regions in the platform at any convenient time, then enable the CICS bundles to verify the installation. When you choose to provide the application version to users, you make the application entry points, and therefore the resources that they control for the application, available to callers.
- Each application entry point is declared on a resource and also names an operation. For example, you could declare application entry points for create, read, update, or delete operations in the application. A resource for an application can only be declared once as an application entry point, naming one operation. You cannot declare multiple application entry points on the same resource.
- An operation name must be unique within an application.
- Operation names are case sensitive, so you may use operation names that are differentiated only by case.

First, you define the policies in a CICS bundle. You then define the scoping for the operation by editing the CICS bundle manifest with the CICS manifest editor to define an application entry point and a policy scope. Finally you add the CICS bundle to a CICS Application project for deployment. CICS bundles that define a policy scope for an operation cannot be deployed with a platform project or added to an already active platform by using the ADDBUNDLE operation dialog.

Policy Scope…

- Configuration example

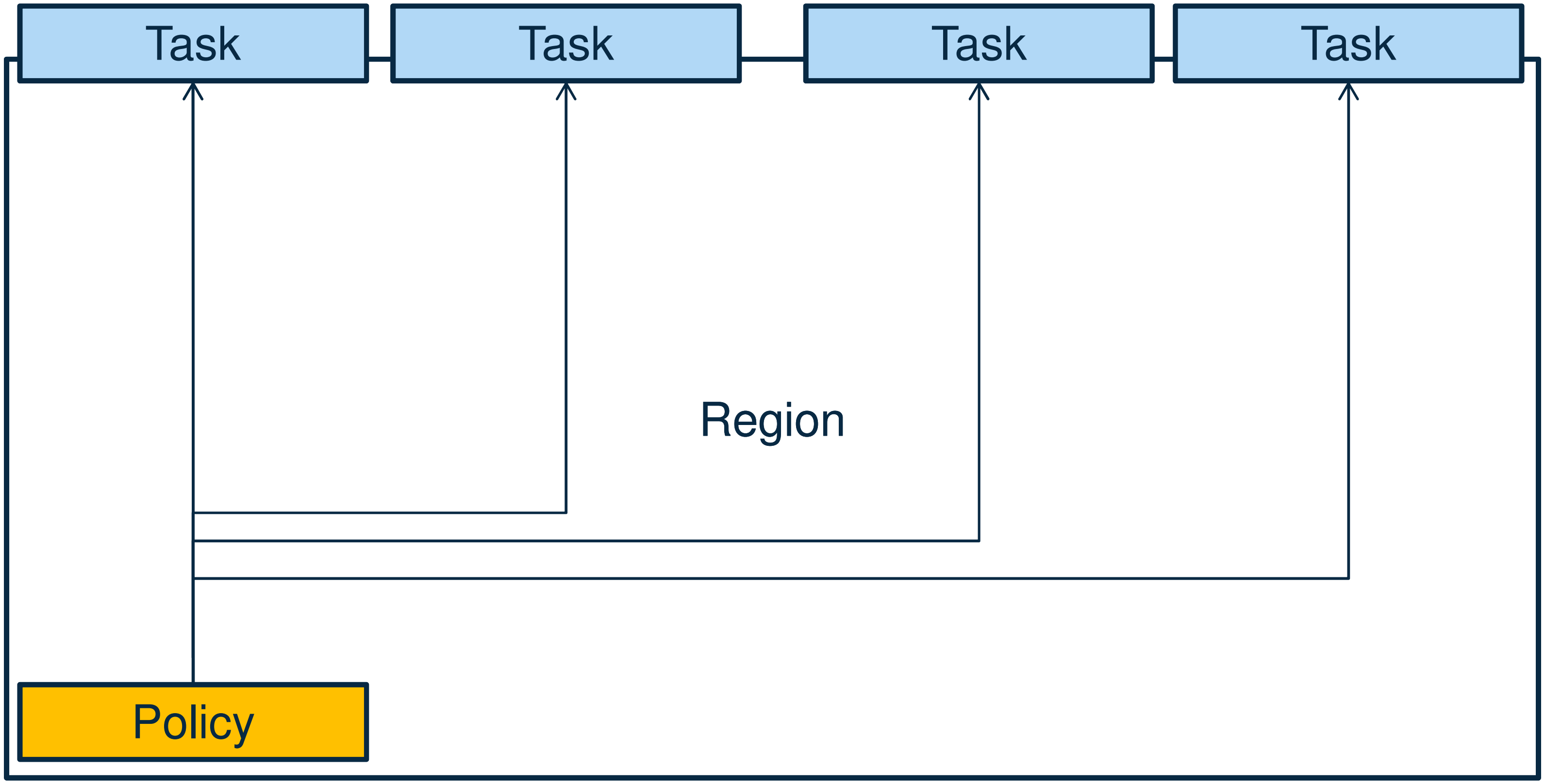


Notes

- An example CICS Platform and Application configuration for discussion of the Policy Scope.

Policy Scope…

- No scope (Region scope)



Notes

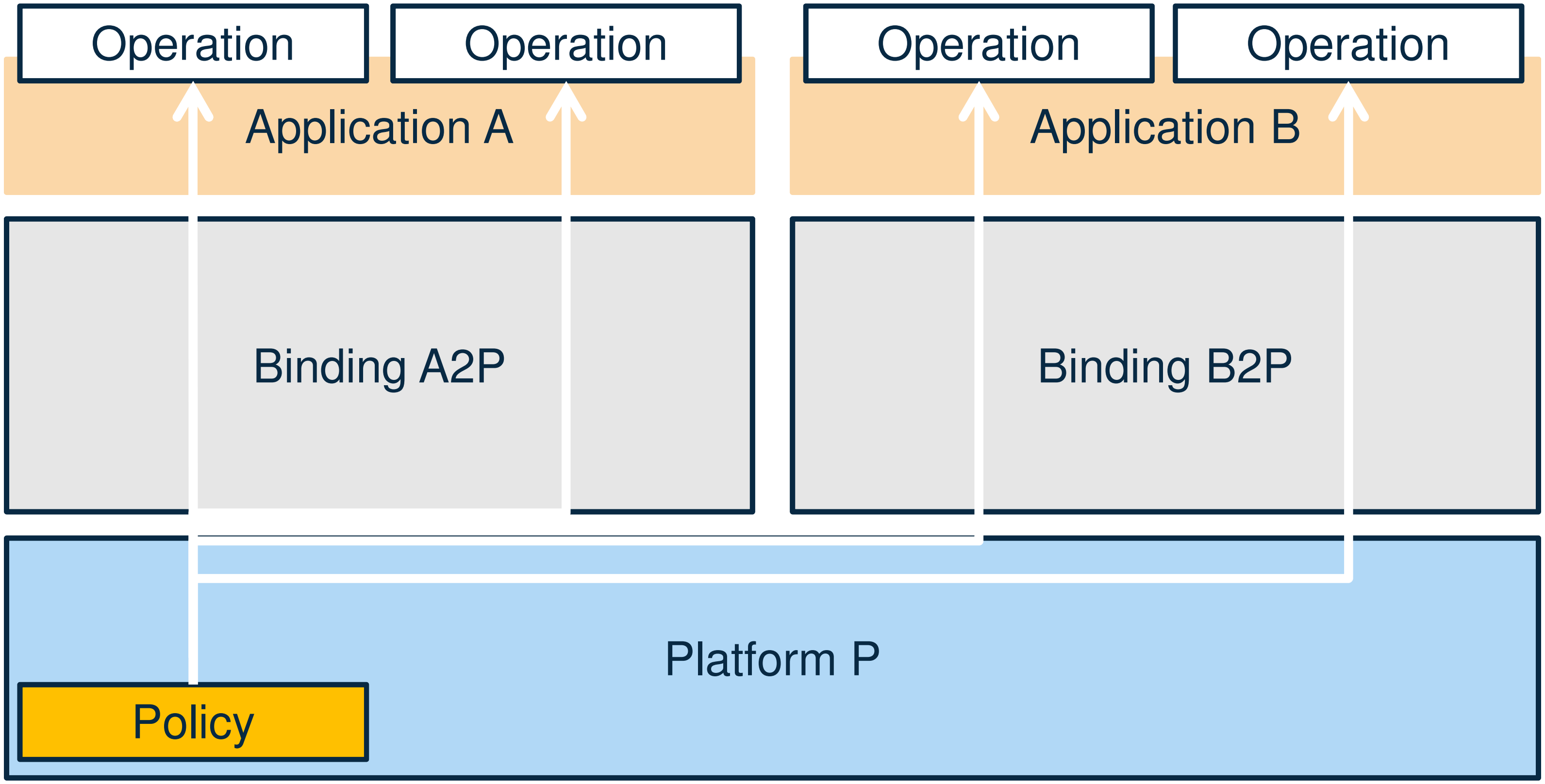
- The policy is deployed as a CICS BUNDLE resource defined in the CSD or CICSPlex® SM data repository, and installed into any CICS region.

  The policy rules apply to all user tasks that run in the CICS region to which you deploy the policy.

- See the following developer works article for addition detail on this topic:
- https://www.ibm.com/developerworks/community/blogs/cicsdev/entry/restricting_the_scope_cics_policies_deployed_to_a_cics_region?lang=en

Policy Scope…

- Platform scope



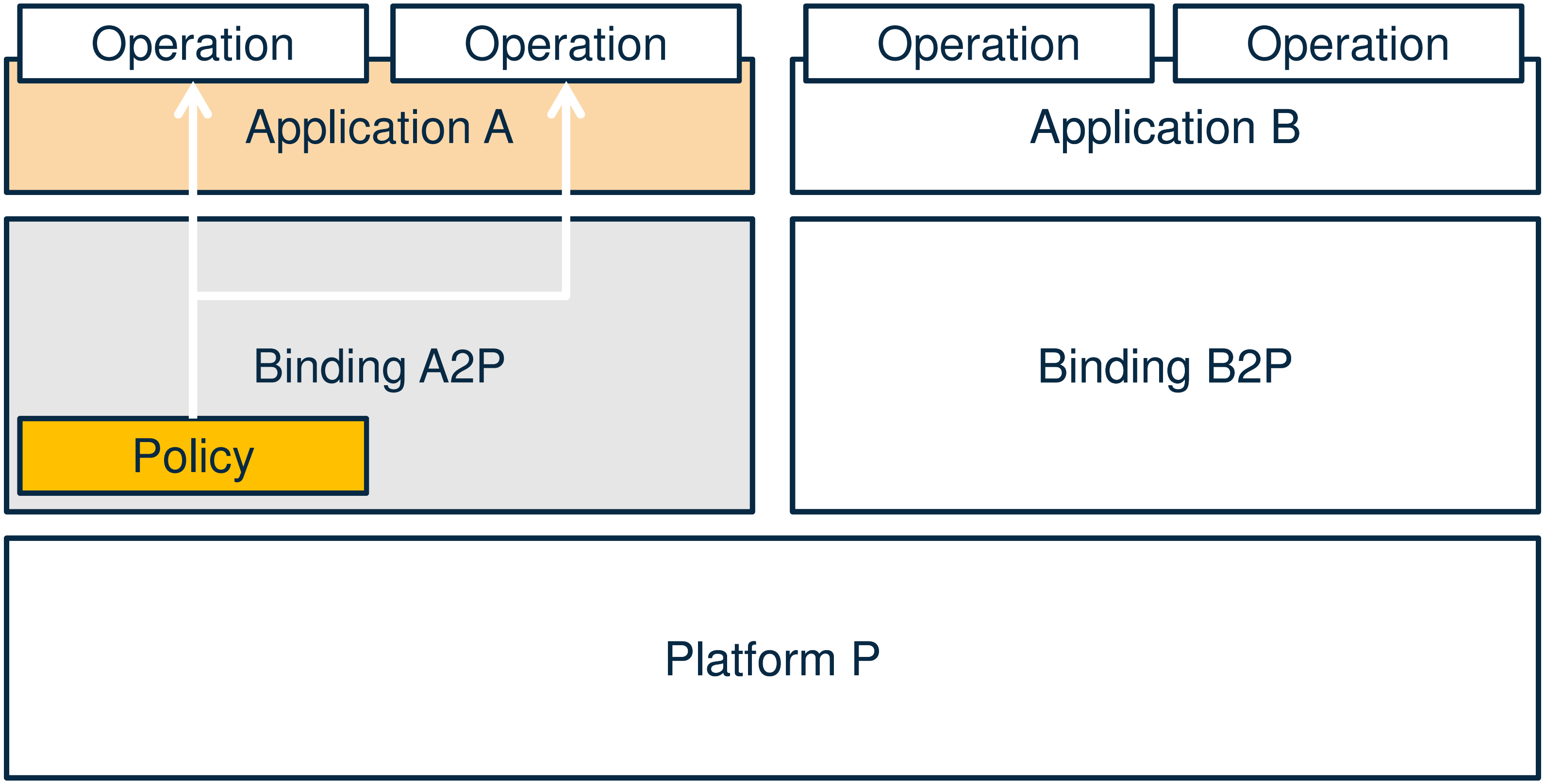
Notes

- When you define a CICS Platform project, you add to it the CICS bundles that contain policy definitions to be deployed with the platform. If you want to deploy a policy to an already active platform, export the policy bundle to the platform home directory in zFS, then use the CICS Explorer® ADDBUNDLE operation dialog to install it into a region type.

- The policy rules apply to all user tasks within the platform that have the matching platform in their application context.

Policy Scope…

- Application scope



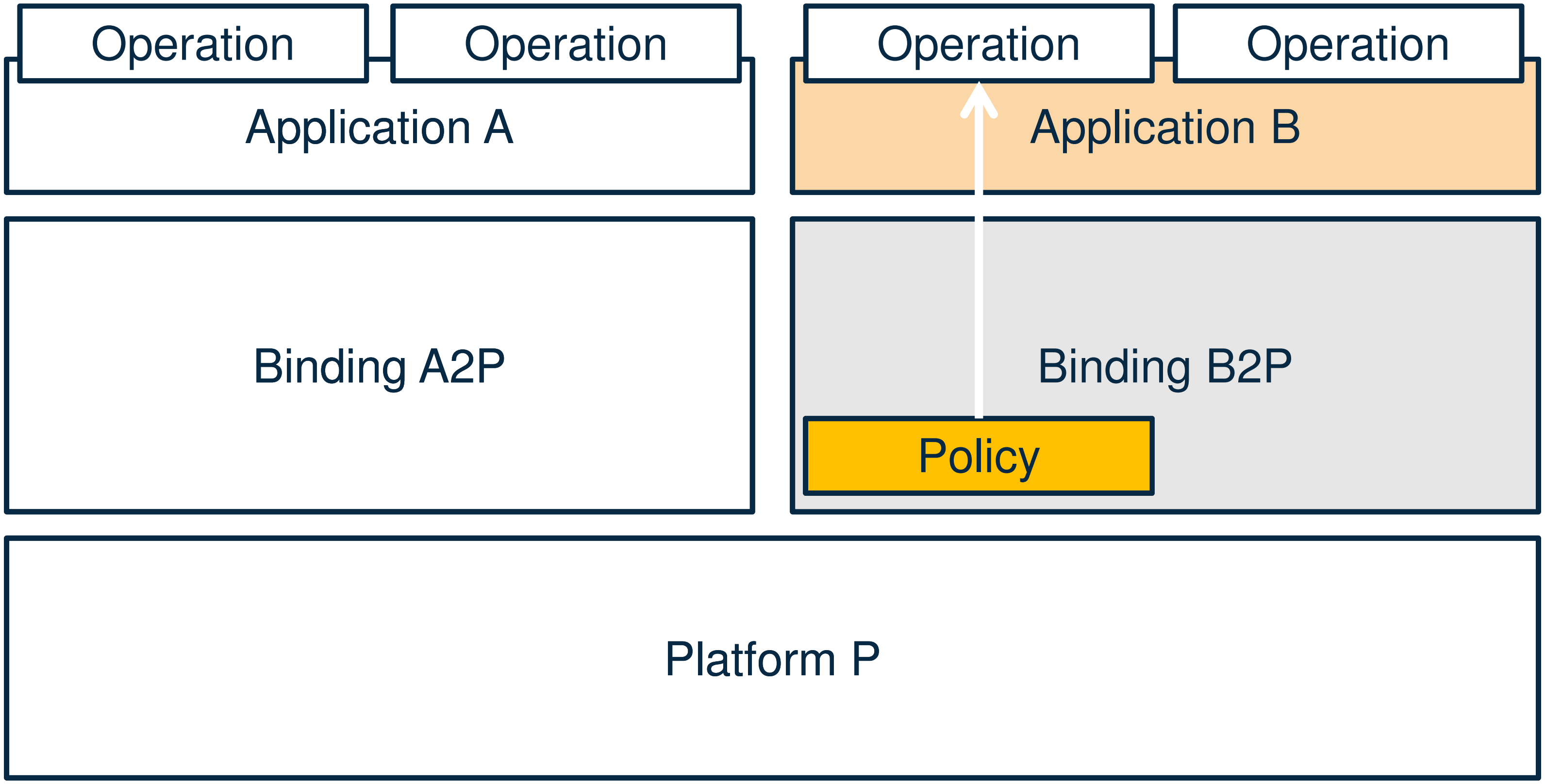
Notes

- When you define a CICS Application project, you add to it the CICS bundles that contain policy definitions to be deployed with the application. Alternatively, you can also deploy CICS bundles with the application binding, depending on the architecture of your application.

- The policy rules apply to all user tasks within the platform that have the matching platform, application, and application version information in their application context.

Policy Scope…

- Operation scope

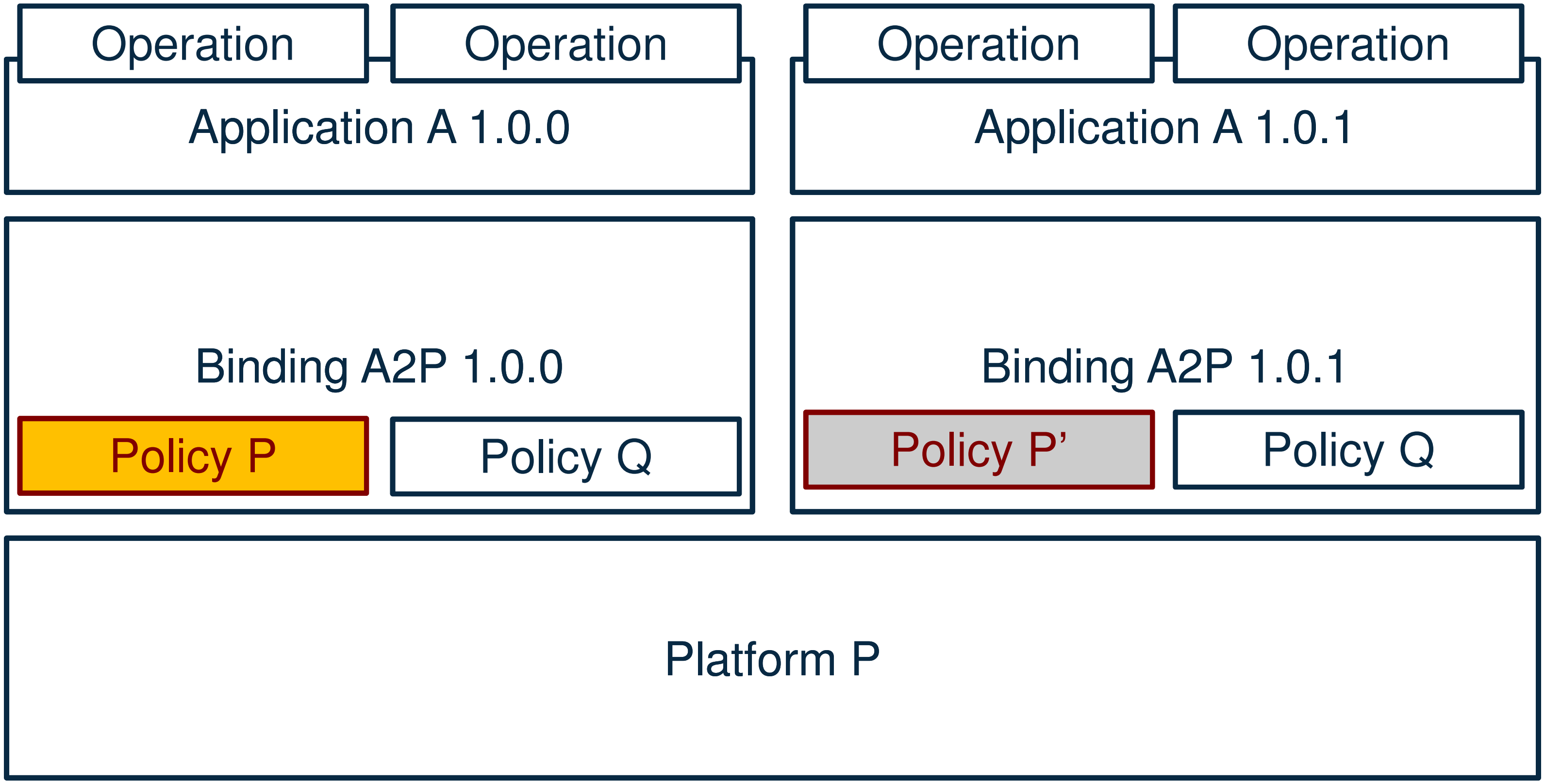


Notes

- The policy rules apply to all user tasks within the platform that have the matching platform, application, and application version and operation information in their application context.

Policy Scope…

- Application scope – Multi-versioning

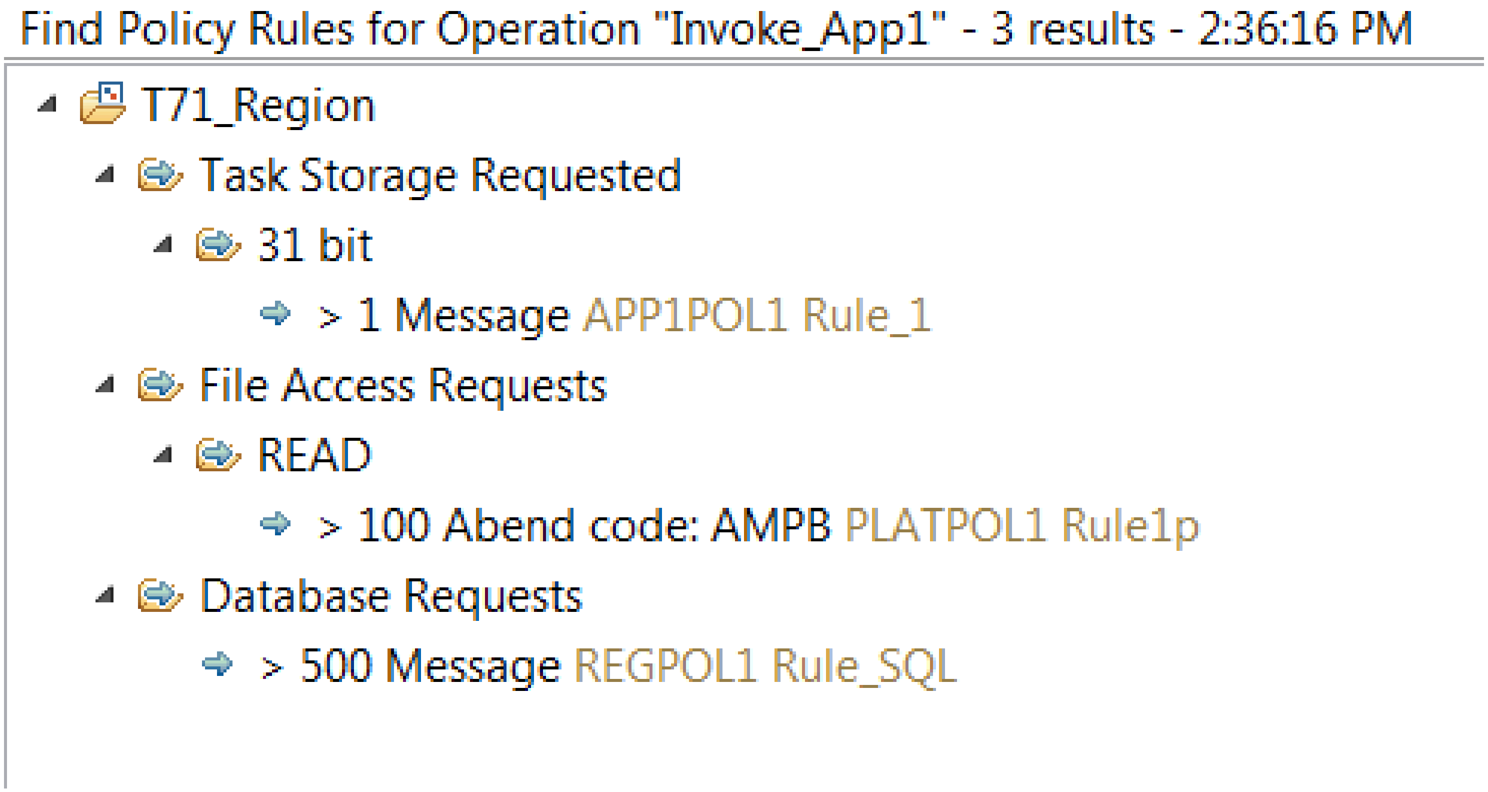


Notes

- An example of multi-versioning an application and changing the policy between the two versions.

Policy Scope…

- An example of a multiple policies being applied



Find Policy Rules for Operation "Invoke_App1" - 3 results - 2:36:16 PM

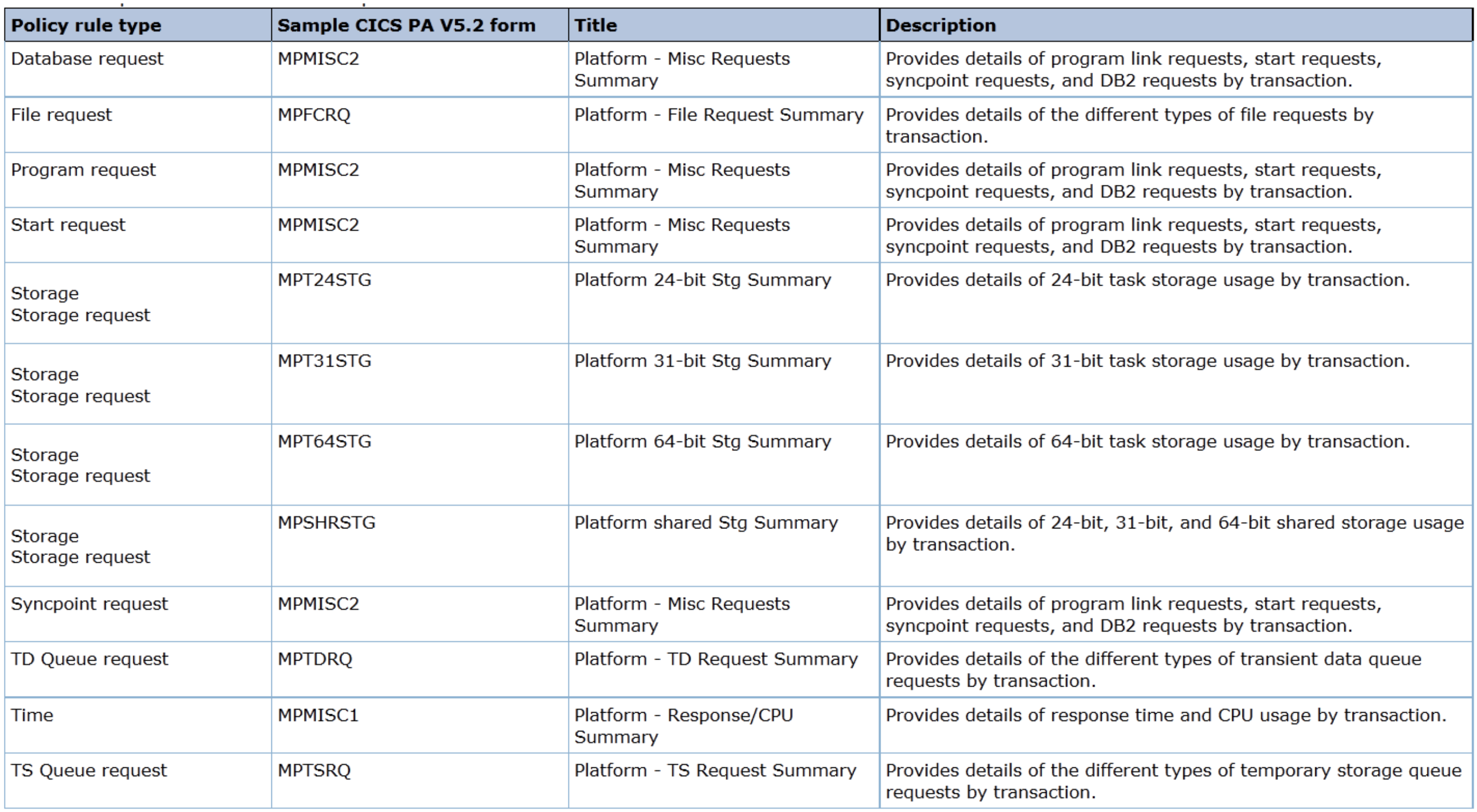
```
◢ T71_Region
    ◢ Task Storage Requested
        ◢ 31 bit
            > 1 Message APP1POL1 Rule_1
    ◢ File Access Requests
        ◢ READ
            > 100 Abend code: AMPB PLATPOL1 Rule1p
    ◢ Database Requests
        > 500 Message REGPOL1 Rule_SQL
```

Notes

- When a policy is installed into a CICS region, CICS combines its rules with all of the other policies that are deployed with different scopes in that CICS region to determine a set of rules that apply for each unique runtime scope. Policy rules that are deployed with different scopes might apply to the same task. You can use the Cloud Explorer view in CICS Explorer to determine which set of policy rules apply to a task.
- If you query policy rules against a specific operation of an application, you see an aggregation of the policy rules that apply. This query shows any additional policy rules that apply to a specific operation of an application, as well as the policy rules that apply to the application.
- If you query policy rules against a platform, you see an aggregation of the policy rules that apply at scopes. This query shows you all the policy rules that apply to all application tasks that run on the selected platform. It is a subset of the policy rules you see if you query the policy rules for a specific application (or application operation) running on that platform.
- Similarly, if you query policy rules against a region type, you see an aggregation of the policy rules that apply at scopes. This query shows you all the policy rules that apply to all application tasks that run in regions of this type on the platform.

Monitoring

- Performance class group, DFHCICS
  - MPPRTXCD
    - » Number of policy rule thresholds that this task has exceeded
- Performance Analyzer 52
  - Sample forms provided for current policies



Policy rule type	Sample CICS PA V5.2 form	Title	Description
Database request	MPMISC2	Platform - Misc Requests Summary	Provides details of program link requests, start requests, syncpoint requests, and DB2 requests by transaction.
File request	MPFCRQ	Platform - File Request Summary	Provides details of the different types of file requests by transaction.
Program request	MPMISC2	Platform - Misc Requests Summary	Provides details of program link requests, start requests, syncpoint requests, and DB2 requests by transaction.
Start request	MPMISC2	Platform - Misc Requests Summary	Provides details of program link requests, start requests, syncpoint requests, and DB2 requests by transaction.
Storage Storage request	MPT24STG	Platform 24-bit Stg Summary	Provides details of 24-bit task storage usage by transaction.
Storage Storage request	MPT31STG	Platform 31-bit Stg Summary	Provides details of 31-bit task storage usage by transaction.
Storage Storage request	MPT64STG	Platform 64-bit Stg Summary	Provides details of 64-bit task storage usage by transaction.
Storage Storage request	MPSHRSTG	Platform shared Stg Summary	Provides details of 24-bit, 31-bit, and 64-bit shared storage usage by transaction.
Syncpoint request	MPMISC2	Platform - Misc Requests Summary	Provides details of program link requests, start requests, syncpoint requests, and DB2 requests by transaction.
TD Queue request	MPTDRQ	Platform - TD Request Summary	Provides details of the different types of transient data queue requests by transaction.
Time	MPMISC1	Platform - Response/CPU Summary	Provides details of response time and CPU usage by transaction.
TS Queue request	MPTSRQ	Platform - TS Request Summary	Provides details of the different types of temporary storage queue requests by transaction.

Complet

Notes

Performance class group, DFHCICS

New performance data field 449 is added to the DFHCICS group:

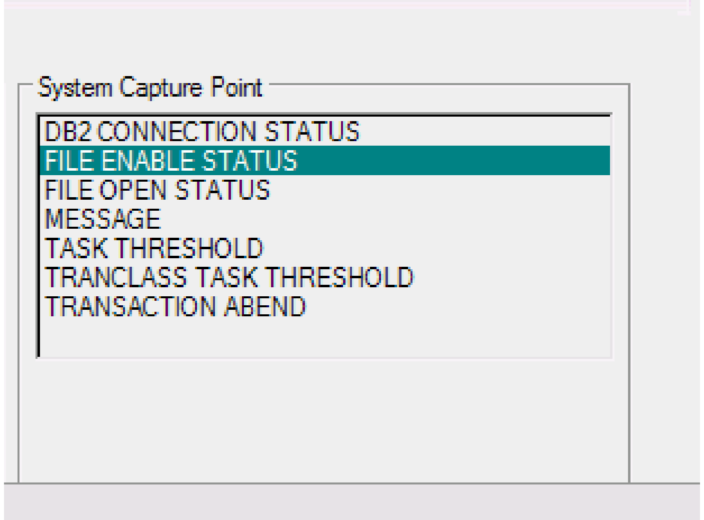
449 (TYPE-A, 'MPPRTXCD', 4 BYTES)

Number of policy rule thresholds that this task has exceeded. This field is all nulls (0x00 bytes) if no thresholds have been exceeded or if the task has no policy rules applied to it.

- You can use sample forms in CICS Performance Analyzer for z/OS (CICS PA) to produce reports that you can use to identify suitable threshold values to set conditions in policies.
- Typically the CICS PA reports list data by transaction identifier. The scope at which a policy is deployed determines whether a policy applies to an entire platform or to a specific application, and transactions that are associated with the application instance.

System Events

- Capture events when:
  - DB2 connection status changes
  - FILE enable status changes
  - FILE open status changes
  - CICS message is issued
  - Unhandled transaction abends
  - Current active tasks for a TRANCLASS goes above or below a certain percentage of MAXACTIVE
  - Current active task in a region goes above or below a certain percentage of MAXTASKs



System Capture Point

DB2 CONNECTION STATUS
FILE ENABLE STATUS
FILE OPEN STATUS
MESSAGE
TASK THRESHOLD
TRANCLASS TASK THRESHOLD
TRANSACTION ABEND

Notes

- A system event is a type of business event that results from system activity and contains system data. System events can include resource state changes, thresholds being crossed, or unusual system states or actions. Use system events to help you understand changes in the state of your system resources or system health.
- You can be alerted to certain CICS® system conditions by capturing events for those conditions. Receiving a notification for any changes to the state of system resources avoids the need to poll for changes after they happen; it also means that you can quickly respond to these system events.
- Event processing supports the following system events: DB2CONN connection status
- FILE enable or disable status
- FILE open or close status
- MESSAGE
- TASK threshold
- TRANCLASS TASK threshold
- Unhandled transaction abend

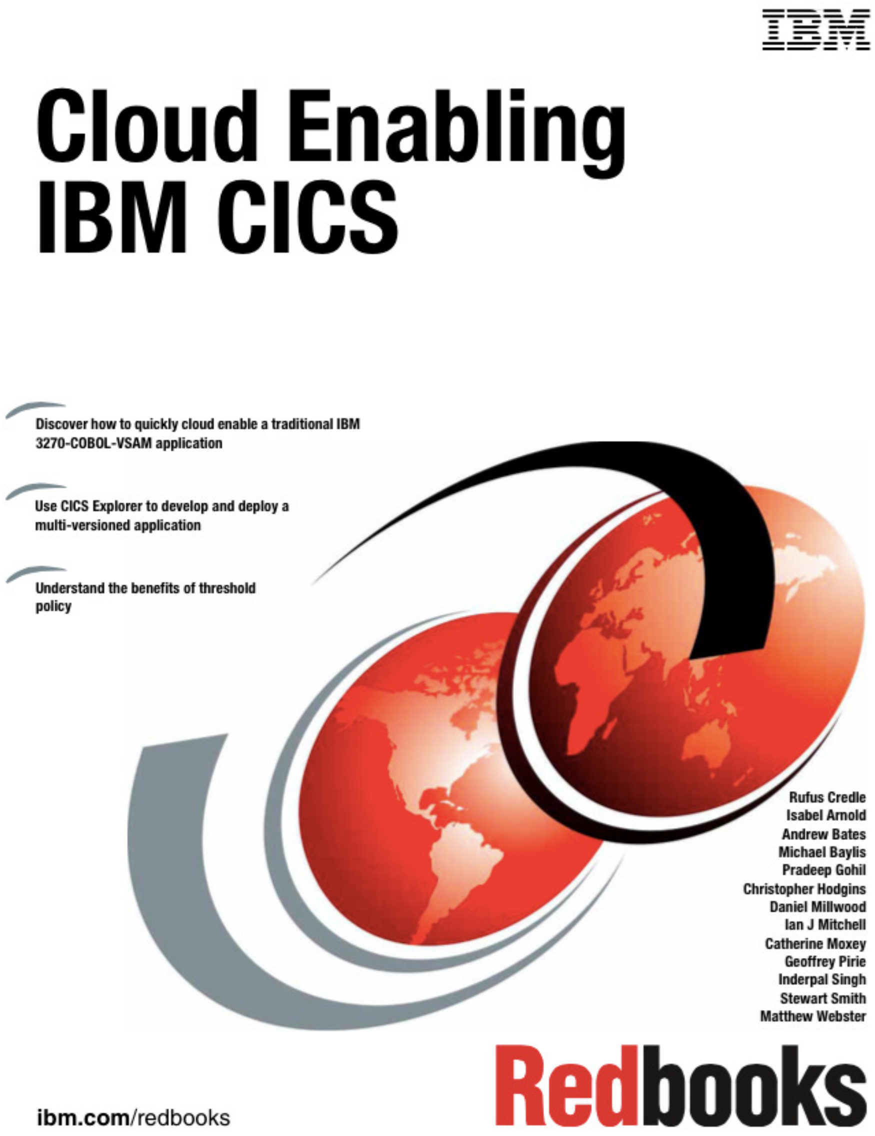
Differences between Policies and Events

- Events
  - Emitted when something of interest happens
    - e.g. Transaction abend
  - Convey information about what happened
  - Cannot control or constrain processing
- Policies
  - Define a contract on how the system/application is to behave
    - Define a boundary within the task can execute
  - Apply to instances of user tasks
  - Can enforce the rules with in a policy
    - Tasks that break the rules are subject to the specified action

Notes

- Policies and events, especially system events, might at first glance seem to provide alternatives that satisfy a common goal, making it difficult to decide which one to use. However, they offer different levels of measurement and control, and are intended for different purposes.
- Policies are there to define a contract about how you want aspects of an application or system to behave. Policies apply to instances of user tasks, and different groups of tasks can share a common set of policies, thus allowing sections of the workload to be controlled in different ways. The collection of policy rules that are associated with tasks that are running in an application or platform define the boundaries within which a task can safely execute. They allow systems administrators to set, in advance, limits on the behavior of user applications. In this way, policies enable CICS to measure, react to, and enforce the behavior of tasks that transgress any of the rules that are defined in the policies that apply to them, as they execute.
- Events fall into two categories: application events and system events. Events are emitted when something of interest happens, either in the business processing that is performed by an application, or in the environment of the system and its resources. Events merely convey information about the thing that happened, they do not control or place constraints on the processing that caused the event. CICS uses event specifications to define the occurrences that are of interest. Events can be emitted to various event consumers, including consumers that run outside CICS, and the consumption of the event is decoupled from the event emission. External event consumers can carry out processing that detects patterns among different events from CICS, or in combination with events from other event producers.
- Events and policies are related in that one of the actions that can be specified in a policy rule is for an event to be emitted; the event notifies an event consumer that the policy threshold is exceeded. In this respect, a policy rule might be regarded as an alternative way of specifying the occurrence that is of interest, for this particular type of occurrence.

Documentation (SG24-8114)



IBM

Cloud Enabling IBM CICS

- Discover how to quickly cloud enable a traditional IBM 3270-COBOL-VSAM application
- Use CICS Explorer to develop and deploy a multi-versioned application
- Understand the benefits of threshold policy

Rufus Credle
Isabel Arnold
Andrew Bates
Michael Baylis
Pradeep Gohil
Christopher Hodgins
Daniel Millwood
Ian J Mitchell
Catherine Moxey
Geoffrey Pirie
Inderpal Singh
Stewart Smith
Matthew Webster

ibm.com/redbooks

Redbooks

Notes

- This IBM® Redbooks® publication takes an existing IBM 3270-COBOL-VSAM application and describes how to use the features of IBM Customer Information Control System (CICS®) Transaction Server (CICS TS) cloud enablement. Working with the General Insurance Application (GENAPP) as an example, this book describes the steps needed to monitor both platform and application health using the CICS Explorer CICS Cloud perspective.
- It also shows you how to apply threshold policy and measure resource usage, all without source code changes to the original application. In addition, this book describes how to use multi-versioning to safely and reliably apply and back out application changes.
- This Redbooks publication includes instructions about the following topics:
- How to create a CICS TS platform to manage and reflect the health of a set of CICS TS regions, and the services that they provide to applications
- How to quickly get value from CICS TS applications, by creating and deploying a CICS TS application for an existing user application
- How to protect your CICS TS platform from erroneous applications by using threshold policies
- How to deploy and run multiple versions of the same CICS TS application on the same CICS TS platform at the same time, enabling a safer migration from one application version to another, with no downtime
- How to measure application resource usage, enabling a comparison of the performance of different application versions, and chargeback based on application use
- This book describes how CICS TS cloud enablement uses existing operational facilities, including monitoring, events, transaction tracking, CICS TS bundles, and IBM CICSPlex® System Manager (CICSPlex SM), to integrate with existing deployment and management processes.

CICS Transaction Server V5.3 open beta

- New Policy Rules
  - Name Counter Server
    - GET COUNTER|DCOUNTER
  - Temporary Storage
    - Support for Shared TS
  - WebSphere MQ
    - Number of MQ requests
  - IMS
    - Number of DBCTL calls
- New Entry Point
  - Transaction
    - Allows association of a policy with a TRANID

Notes

- The CICS Transaction Server V5.3 open beta adds new policy rules and an new entry point.
- The IMS policy is enforced in the CICS/DBCTL task Related User Exit. Unlike the other thresholds this
- policy will count requests in a Data Owning Region, if the DLI request is function shipped, not in the Application Owning Reion.

Summary

- CICS Policy Based Management
  - *Allow you to set thresholds on the resources that your applications are allowed to consume*
  - *Allow you the ability to notify, to react, or to ABEND rogue tasks*
  - *Allow you to define the scope of your policy rules*
  - *Give you capabilities to protect and control your CICS systems*

Notices and Disclaimers

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Notices and Disclaimers (con't)

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

- IBM, the IBM logo, ibm.com, Bluemix, Blueworks Live, CICS, Clearcase, DOORS®, Enterprise Document Management System™, Global Business Services ®, Global Technology Services ®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, SoDA, SPSS, StoredIQ, Tivoli®, Trusteer®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.